Industrial Security & Compliance

Leveraging Pacesetter Experiences

Rick Kaun
Manager of Industrial Security & Compliance
Matrikon, Inc.

Introduction: State of Industrial Security

Market competition in industry has traditionally driven the evolution of control systems. Over a decade ago, most control systems were autonomous and built upon proprietary vendor technology and the solutions were geared towards access to data, speed, and functionality (or reliability). The most important feature was access to data. At first many vendors built their own protocols or languages to allow for the transfer of data and soon the automation landscape became very proprietary and independent of other systems and protocols. Parallel to this was the development of Ethernet networks for business data networks. In early 2000, vendors saw advantages to include 'Ethernet-compliance' to allow for communication between systems including those outside the plant environment. However, in the rush to market many vendors built ad-hoc versions of protocols that worked for the purpose at hand but did not include security.

Now most industries with control systems[1] are facing many pressures to both allow access to data and to secure it. There are many forces pushing these opposing trends including data access to enable business decisions, vendor access for process improvements and advanced control exercises like loop tuning and alarm management, as well as for proving regulatory compliance. However this increasing need for access is further diluting the security of many of these systems and is putting many process control environments at risk. In some industries this is more of a nuisance than anything, but for most industries a loss of control over your process can mean a serious safety threat. As one noted security professional who works for a major refinery once pointed out, “our industry is one such that a loss of access or control over our systems usually means someone dies”. Regardless of the potential harm, any industry with little or no security in and around their control system will at least lose production for some time. This can translate into re-work, overtime, environmental release, and other intangibles such as competitive edge, investor confidence and potentially the ability to stay in business.

The new push for control systems is to try to balance the two opposing trends: Access and Security. And the pressure is coming from many angles. Increasing market competition means that most industries are 'pushing the envelope' to run faster, more efficiently and with less downtime. This means more outside 'tuning' and better visibility into production from specialized experts who may not be physically at the site. The advancing age of the workforce in general means many industries are automating more control of their assets and expecting the same staff to manage & optimize more resources thereby increasing their reliance on computers. More often than not these computers are running a Windows platform which means all common threats usually targeted at corporate and business machines are now a potential threat to the production environment. The challenge is that traditional IT 'best practices' can't always be applied to control systems without breaking the applications that are running on those systems. For example, the use of antivirus and patch management tools can often break the applications they are designed to protect. In these cases the challenge is to find a way to make process control environments as secure as possible without breaking the control systems along the way.

Security Pacesetters – What are they doing?

The scope of the term 'security' often seems vague and the sheer volume of effort and areas of concern this may represent can be overwhelming. However, this need not be the case. In looking at a number of security frameworks or standards a common theme emerges that is quickly being adopted as a holistic and effective approach to security. This approach combines efforts and initiatives that go far beyond the purchase and deployment of technology. Different initiatives, such as the SP99 from the ISA or the CIP 002-009 from the NERC CIPC, offer different sections, headings and names for each of their areas of concentration but in the end, all efforts can usually be summed into three (3) foundational areas: People, Processes and Technology. The rest of this paper talks about each of these areas in detail, as well as the priority of developing a security philosophy which will in turn foster a security culture. Underpinning all efforts within your organization you must first have a security philosophy and always work towards creating and maintaining a strong security culture or your momentum will be lost.

[1] For the purpose of this paper control systems refer to both distributed control systems, or DCS, as well as SCADA systems since they face many similar challenges

Security Philosophy

Before beginning any security program or initiative your organization must first adopt a security philosophy. A security philosophy will sound different for each company, industry and region in which it is created but there are some basic requirements that all security philosophies must have.

Security is Important

The first premise is quite simply that security is important to the organization. This means the decision makers, the owners and operators of the systems, the support staff, the consultants, vendors, site staff, in short everyone, understands that keeping your facility secure is in everyone’s best interest. This is no different from the importance placed on safety. More often than not, an industrial facility has a long history of always trying to raise safety awareness and tried to educate everyone as to why safety is important. Every employee, contractor and visitor onsite needs to have safety orientation and updated each year. This also needs to happen for security, and can be integrated into safety programs. Without rank and file team members who understand their role and the importance of their actions (or inaction) at your site, you will not succeed in securing your facility. It is a harsh reality but the simple fact remains that your internal, trusted employees have the greatest opportunity to cause or create a security breach intentionally or otherwise. In other words, your security program is only as effective as your least informed employee.

Security is On-Going

More often than not, many organizations see security programs or initiatives as projects that have a defined start, finish and cost. This may be the case for a particular component of your on-going security efforts, but true, lasting security is an on-going initiative. This is quite simply due to the fact that security concerns are brought about by technology - and technology keeps changing! What was a threat yesterday or last week may be fixed by your current firewall rules or Antivirus definitions, but the next threat coming will not be as deterred. Less than 5 years ago USB keys or ‘thumb drives’ were an emerging fad. Today they are sold more cheaply than ever, are capable of huge storage capacities and require little or no knowledge of specialized applications or programs for using them. Another example is the explosion of web-based applications. More and more DCS-level equipment is being sold with HTTP services being installed at the control level. This was not a concern a few years ago. Unfortunately your security program is only as effective as it is current.

Security is Everyone’s Concern

This topic is the basic premise on which your security philosophy needs to be built. As mentioned earlier, your weakest link and biggest threat is your least educated employee. If you install security programs, risk management processes and a healthy business continuity plan or disaster recovery plan you are well on your way to securing your environment. However, if any of those efforts cause a change in the day-to-day business flow for your employees then you will need to explain to them why these changes are necessary. Too many times are programs implemented without the proper awareness training and education for the people whose daily lives are most affected. In these cases it is only a short time before the day-to-day users start to find ways around the new systems you just put in place thus negating your efforts. Think of a school computer lab where students are some of the most creative people at bypassing security because they do not understand or care about security. Your security program will live and die based on how well your employees receive and embrace it.

Security is a Balancing Act

The last and perhaps most important thing a proper security philosophy needs is the attitude of balance. In this sense the balance is between risk and reward as well as between effort and return. In order for your organization to move toward a proper security program you must first decide as an organization what level of risk you are willing to live with. Every change you make to your current environment towards security is going to cost something whether it is time, money, or access to your data. And no matter how you do proceed, there is a very good chance that you will still have some sort of incident at some point in time. A security incident can be catastrophic system failure or subtle inappropriate access to data or an IO room. The true measure of your security program will be in how well contained the incident is, how quickly you recover, and if you choose to learn and benefit from it.

People – The Biggest Risk

The first thing a security pacesetter will do to address the human factor of security is to create an internal advisory group to address social issues. This group should have a representative of each logical area of your facility as well as someone from each level of management. This means that everyone from the site manager or executive level down to the administrative department needs to be represented on this panel. The panel shall operate as a higher-level group and will be responsible for disseminating information between site staff and other groups. This will allow for quick propagation of information and awareness and will aid in the smooth and seamless adoption of new initiatives as they develop.

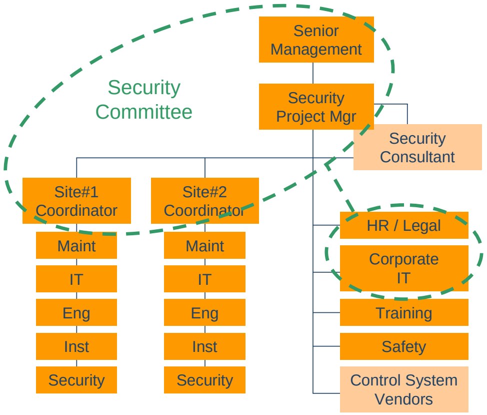

Figure 1 - Security Organization

Awareness Programs

An equally important initiative in this scope is the creation and distribution of awareness programs. For specific industries facing specific security regulation (i.e. CIP 002-009 for Power)[2] the awareness program can be specifically tailored to timelines and schedules of the standards' adoption and implementation. For other industries the focus can be on general security awareness as part of the corporate emphasis and consciousness. In either case by getting the employees aware of the timing and importance of the subject and its subsequent initiatives and projects within your organization you will have better adoption. Security is a huge change management initiative affecting corporate culture.

Training

A third component of your security program is the notion of training and cross-training your people. The specific steps and procedures required to make use of new technology or of changes to the way people do their job needs to be rolled out. Examples can include the adoption of a new VPN client and rules about it use. While this usually can be captured in a document and appended to an e-mail, an end user training of the tool and how it is to be configured is much more effective and safe.
Further, cross-training of specific individuals and frequent drills within a department as to the security procedures and processes is also very important should you have a security breach or need to restore a system or react to an incident. Too often the security burden or the 'IT' person in the plant is a team of one (1); with most of the security knowledge buried in his brain and not on paper. This is a significant risk to your organization if you have all the knowledge of the control system in one person's head.

Process

One of the most obvious indicators of the success or failure of your security effort is reflected in your processes, standards, guidelines, procedures and best-practices. Timely response to incidents, which is inevitable, is measured by how well you contain your problem, how quickly you recover to full operation and

[2] The NERC CIP standard requires both an executive level sponsor for security as well as awareness & training programs.

how much damage was done are all indicators of the effectiveness of your processes. To fully secure and protect your organization there are literally dozens of policies and procedures you can implement, but the for sake of this discussion the four (4) most significant are examined below.

Disaster Recovery

Disaster recovery (DR) is a very important procedure to develop in your security efforts. Many businesses balk at the sheer magnitude of a corporate-wide DR plan due to complexity, costs, and effort required to plan and implement it. However, system-specific or machine-specific DR plans are easier to implement and are much more practical to implement. At the very least you should try to create plans for recovering or restoring your most critical assets in your first year, then as you progress with your security plan you can expand the scope to include less critical but still integral components of your network infrastructure. However, it is not enough to simply create the plan or to take an image of the machine for future restoration. To ensure your plan works or that your systems are properly backed up you must test the restoration or recovery of your system at some time as part of your DR plan.

Back up and Restoration

This is the cornerstone of any security policy. An effective backup plan must include regular, periodic images of your core systems and data sources. In addition to system builds, with the use of imaging software, and data repositories critical to operations, a robust backup procedure will include backups of system states, multiple versions, restoration points and a logical rotation of storage media that is stored in a separate physical location from your site. Further, it is important that as part of your fire drill and response handling you create a regular test whereby you audit the site (third party or in-house) that your media is stored and that you test the method by which the media is retrieved and put back onto your restored systems. There have been instances in the process control industry in which the third party storage location has been compromised or in which the retrieval of the backup media was not available on a 24 X 7 basis under which critical systems operate. If your system must be up 24 hours a day then access to the backups for that system must also be unencumbered.

Incident Handling

The true measure of your security readiness is going to be how well you handle an incident when it happens. As introduced above, an incident **is** going to happen at some point regardless of how well you prepare or how hard you try to avoid it. What counts is how much damage you can avoid by early and effective detection and mitigation with countermeasures. In other words, the sooner you see the wound and the faster you can stop the bleeding, the more effective your policy is. Processes which facilitate incident handling include (among others) team notification, escalation procedures during an incident, containment procedures (for slowing or stopping the spread of viruses), interim measures for resuming business and post-incident analysis.

Fire Drills

Fire drills are the potentially the most important aspect of your processes. Some entities spend a lot of money, time and effort on creating and implementing procedures for protecting and backing up their critical assets. However not enough of those companies effectively test those processes and they may subsequently be out of date and not longer suitable. Too many times clients have backed up critical data and machine images to external tapes only to discover that when they needed to access the tapes, the backups did not work or the tape was corrupt. Similarly, many businesses create valid tapes and storage media but never try to implement a recovery scenario until they are in the midst of an incident. Unfortunately, for many of these entities this is the first time they try these procedures and they painfully learn that what makes sense or what sounds logical in the planning stage does not necessarily transpire in reality. In the end many businesses quickly discover that the best laid plans do not always add up to real-world stress testing. By implementing a regular testing of any process that is not part of standard operating procedures you will quickly discover any weaknesses in your overall security plan.

Standard Deployment

Once you have put all this effort into creating a secure environment you need to maintain that in the face of future adds moves and changes to your network. The simplest way to do this is to create a base-line standard for systems that get put into production at your facility. This baseline then gets shared among your sites/departments/locations as the basic security standard for all systems both existing and new. The creation and adherence to such a standard means that future projects will continue to enhance your security profile rather than break it down. This particular process is one which is interdependent on your security culture. The effort required to create and maintain a standard needs to be supported by your organization. The flip side is that the presence of a standard which everyone must be aware of and adhere to helps to further your security culture. In essence your standards and your security culture work together.

Patch Management

Perhaps the single most talked about process within industry when talking about security, no program would be complete without a patch management process. Some industries make use of a team which reviews all new patches released that are in scope for their facility. They then look at the impact the underlying vulnerability would have on their systems and rank the urgency for the patch to be deployed. The urgency ranking then corresponds to the time-line allowed (internally decided) to test and install the patch. The patch itself is first tested on a non-production system to ascertain the impact it will have to the production environment. Once the testing is complete, the patching team then notifies system owners of the desired schedule to deploy the patches to the production environments. And if the patch does not pass the testing phase due to a negative impact to the system it is being installed on, the patch team researches alternatives to the patch. For example, some vulnerability can be mitigated through the disabling of particular services or ports on the target machine or within the network it resides. Whichever method your facility is prepared to take (installation or mitigation) a well thought-out patch management process and dedicated resources to carry it out are very important to minimizing the risk to your network.

Technology

Perhaps the most obvious and fundamental piece of the security puzzle is the technology aspect. Technology is an enabling, tangible aspect to any security program. However, simply buying and installing the technology does not necessarily increase your security profile. Your technology investments must take into account your business model as well as your physical topology and your plant or operational requirements. This section discusses three (3) of the more important aspects of security from a technological perspective.

Defense in Depth

The first word that comes to mind when discussing technology and security is a firewall. This response is both good and bad. On the plus side the fact that your organization may already be, or is intending to use, a firewall means that security is a priority and that the potential for locking out unwanted access exists. The problem is that many organizations feel that the mere presence of a firewall is enough to immediately solve their security concerns. In a recent study of 37 firewalls from a number of industries it was found that "…almost 80% of firewalls allow both the 'any' service on inbound rules and insecure access to the firewalls these are gross mistakes by any account."[3]

To deploy a firewall properly in a security model an organization must make effective use of the technology. Purchasing a firewall and then opening multiple high-risk applications like SQL/www, or allowing the 'ANY' rule inbound for connections simply renders your firewall towards the realm of an expensive 'bump in the line' and away from a security tool. For the maximum firewall benefit, industries need to create a multi-layered topology in their process control network. This approach has been called a 'defense in depth' approach or a 'secure process environment' but regardless of what you call it, the further removed your process network is from your business LAN and the outside world (i.e. The Internet) the more protected you

[3] A Quantitative Study of Firewall Configuration Errors" Avishai Wool, IEEE Computer Magazine, IEEE Computer Society.

are. More importantly you need to establish what traffic you WILL allow on a frequent basis and ensure that future projects in your facility do not compromise those rules. Every few months revisit the firewall configuration to ensure it is working effectively and addresses new security threats. There is always a second way to move data or to facilitate business decisions without compromising your firewall which is your first line of defense.

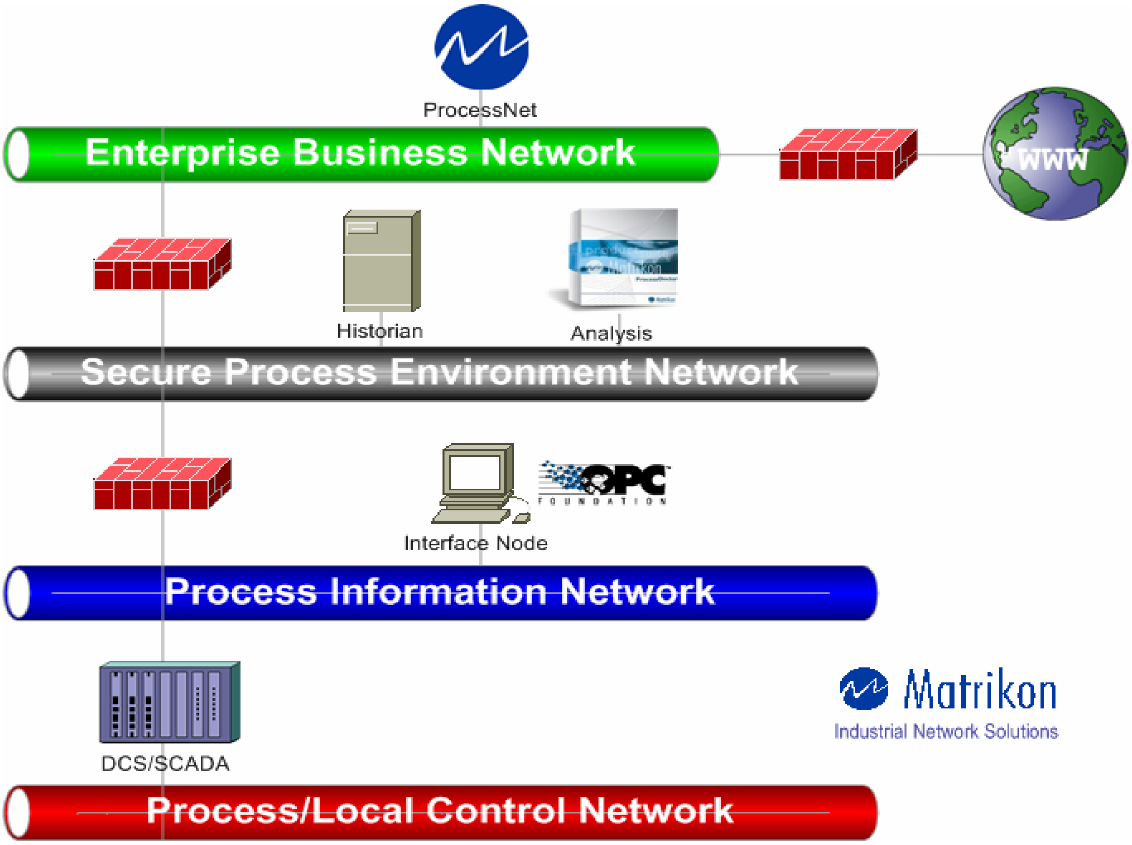
ProcessNet
Enterprise Business Network
WWW
Historian
Analysis
Secure Process Environment Network
Interface Node
OPC FOUNDATION
Process Information Network
DCS/SCADA
Matrikon
Industrial Network Solutions
Process/Local Control Network

Figure 2 – Secure Process Environment

Secure Administration Gateway

As more and more industries face the need to secure their production environments but still permit access to outside parties such as consultants and vendors, new solutions must emerge. One such philosophy is to implement a Secure Administration Gateway (SAG). An SAG, like a firewall, is more of a philosophy than a technology or appliance. In other words, no matter how you choose to implement it the principle is one of controlled, auditable central administration over access to your critical control network. SAG acts as an electronic central gate through which all access must pass. This includes internal employees, corporate or otherwise, as well as third parties, vendors, consultants, and traveling or remote trusted operators. If SAG is properly designed and deployed it can hook into your Active Directory or RAS server, it can log all activity including screen captures, keystroke logging and anomaly detection should you so desire. The benefits of SAG to controlling access and to log that access are immense especially in situations where access must be logged for regulatory expectations, traced & steps reversed, or where a large number of assets/systems are the responsibility of a small number of operators.

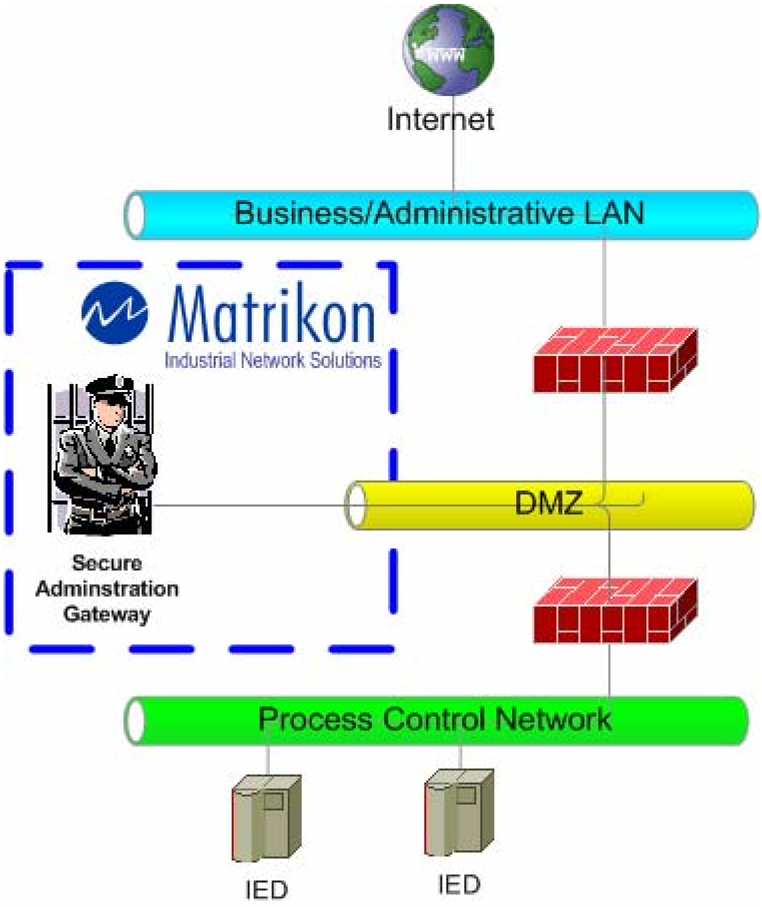

Figure 3 – Secure Administration Gateway

Annual Security Assessments

While this is not a technology itself, it is a test of your existing technology. And as more and more companies put security programs in place there is an increasing call for testing the technology once it is implemented. One example of annual testing recommended by many organizations and standards is an annual (or regular) penetration test. The problem with penetration testing is that your exterior wall is only the beginning of your security profile. You may pass an external probe test but if your organization has little or no control over the people and processes inside the organization, or if the entire network is available once inside the perimeter, then you need not be concerned with the enemy at the gate.

Recurring security or vulnerability assessments which test all aspects of your security policy (i.e. People, process AND technology) are key to your continued security efforts. Technology is always changing and as such you must always review your entire security program from policy reviews to access logs to the general scope and mandate of your security initiative.

Detection and Monitoring

Much discussion takes place about the effectiveness or use of Intrusion Detection and Monitoring systems. The benefit of such a tool is the ability to detect intrusions as they happen. The biggest drawback to such a tool is the cost both monetary in the installation and procurement phase but also in the on-going use. It is estimated that in the Power industry alone, the component of the CIP standard that refers to Intrusion Detection would cost from $50 000 to $500 000[4] per utility depending on the size of the site. Multiply this by

[4] http://www.trustednetworktech.com/documents/TNTUtilitySurveyIssuePaper.9000.081005.pdf?market=tnt

the 3100 utilities in the US and the potential spending on Intrusion Detection for CIP compliance ranges from $155M to $1.5B dollars. And this is just the procurement phase and does not include cost of ownership. This does not mean Intrusion Detection is only for the rich and has little benefit. It simply means that to include an effective Intrusion Detection program you will need to be prepared to commit significant resources to the effort. The benefit is that you do not just build a huge, electronic perimeter and allow free, un-guarded reign once inside your network. There are very real benefits to monitoring.

Becoming a Pacesetter

The single biggest differentiator that sets a pacesetter apart in the world of industrial security is their security culture. Any security initiative is going to live and die by the support it gets outside of the project team implementing it. This means financial support for the time and resources required to implement the project itself. It also means support from the executive and decision makers in allowing and encouraging security efforts in the first place. Most importantly it means getting the ‘buy-in’ of the day-to-day owners of the systems being impacted by changes to processes or procedures required to increase security. And the amount of support shown towards security is the key indicator towards the adoption and therefore the success of any security initiative. This is not an easy task to accomplish since security has traditionally been seen as an expense with no obvious ROI. However, if security culture and security systems are thought of in the same light as your safety systems then the opposition to security programs should begin to fade. Safety programs have provided benefits to organizations, and security can provide unintended benefits as well once you get started!

Rick Kaun is the manager of Matrikon's Industrial Security and Compliance group. He leads a team of experts who specialize in computer network infrastructure and risk management with an emphasis on security. Rick has both a Network Engineering Technician Diploma and Bachelor's degree. He is active in alumni activity, is a frequent guest lecturer and participates on the NAIT Network Advisory Committee. Rick also participates in NERC's CIPC meetings and contributes to the development of security guidelines within NERCs Control Systems Security work group.

- Northern Alberta Institute of Technology, Canada
  - Network Engineering Technology (NET), April 2001.
- Alberta Society of Engineering Technologists (ASET) – Certified Computer Information Technologist (CCIT)
- Control Systems Security Working Group (CSSWG) Participant – Working group of the North American Electric Reliability Council (NERC)
- Process Control Security Forum (PCSF) Participant
- NPRA Cyber Security Committee participant
- Certified Information System Security Professional (CISSP), In Progress

rick.kaun@matrikon.com
+1 (780) 945-4055

Matrikon delivers solutions for Operational Excellence through enterprise-wide access to real-time information. Our track record says it all -- integrating plant automation hardware, providing data and system connectivity, security, advanced applications for maintenance and control, asset management, and Web-based decision support applications for the world's leading mining and mineral processing (M&MP) companies since 1988.

We enable your key decision-makers to easily access all the information they need: Web-enabled, secure, and in real time. Matrikon provides total visibility for your plant operations and business processes, so you can back your decisions on single-source information and on fact, not speculation.

With offices in major cities throughout North America, Australia, Europe and the Middle East and a global client base including industry leaders in a wide range of industries, Matrikon’s reach is global.