IT/OT Convergence

Bridging the Divide

Derek R. Harp
Bengt Gregory-Brown

NEX DEFENSE

CONTENTS

1. Abstract 2
2. The Problem 3
   A. Statement 3
   B. Change Drivers – Why Converge? 4
3. Challenges 6
   A. Technical 6
      i. Environmental 6
      ii. Compatibility 6
      iii. Skills Shortage 7
      iv. Security 8
   B. Organizational 9
      i. Business Silos 9
      ii. Culture Clash 10
      iii. Risk Tolerances 11
4. Solution 13
   A. Leadership 13
   B. Planning 13
   C. Testing 14
   D. Education 14
   E. Observation 15
5. Conclusion 16

Bibliography 17
APPENDIX A: Selected OT Disruption Incidents 18
APPENDIX B: Terms and Definitions 19
Contributors 19
Author Bios 20

1 ABSTRACT

Information Technologies (IT) and Operational Technologies (OT) have long, isolated histories with many examples of failed attempts to integrate them or even use tools from one environment in the other. This paper discusses the reasons for this situation and how they relate to the challenges of convergence. The authors attempt to define the problem and outline several aspects of its successful resolution.

This paper draws many of its examples from the energy, oil & gas, and financial industries, as these are widely considered the most vulnerable and disruptions of their operations to have the greatest and most immediate national impacts. The difficulties discussed and the recommendations made are equally applicable to all industries using OT.

2 THE PROBLEM

Statement

Operational Technology (OT) consists of hardware and software systems that monitor and control physical equipment and processes, often found in industries that manage critical infrastructure, such as water, oil & gas, energy, and utilities, but also in automated manufacturing, pharmaceutical processing, and defense networks. It even forms the foundation of building control systems, air and road traffic controls, shipping systems and, increasingly, management of distributed data storage and processing networks, i.e., cloud services.

This technology uses many specialized terms such as process control domains (PCD), programmable logic controllers (PLC), distributed control systems (DCS), supervisory control and data acquisition (SCADA) systems, safety instrumented systems (SIS), and building management/ automation systems (BAS), often collectively referred to as Industrial Control Systems (ICS).

While the technology is familiar to operators and engineers in these sectors, there is limited understanding outside of people working in or with these specialized environments. In contrast, Information Technology (IT), managed by CIOs and IT departments, is the application of computers to process, transmit and store data, typically in a business or enterprise environment. Historically, OT and IT have not overlapped and were managed as separate organizational silos. However, since the turn of the century business demands and economics have changed this. For example, in the energy sector the introduction of real time energy trading markets and demand response have necessitated the need of a certain amount of convergence.

However, the disconnect between these critical units has generated unreliable outputs over the past few decades, and the significant benefits of convergence, such as insight into security risks and enhanced performance, demand attention across the technology landscape.

Traditionally OT elements such as ICS have had long lifecycles compared to IT, which has seen tremendous relative and absolute gains in its areas of focus, namely data storage, processing and communications. The majority of progress that OT has made has been in proprietary systems, which are difficult to scale across multiple technologies and providers. In order to reduce development and support costs and reduce time to market, OT vendors have integrated many IT-derived developments and will continue to do so, but the path is uncertain and the potential impact of missteps is tremendous. OT and IT certainly have significant hurdles to overcome in pursuit of collaboration, none greater than the challenge of achieving security and interoperability without disrupting critical services or diverting excess capital from the enterprise.

Change Drivers – Why Converge?

With labor costs perennially on the rise and a growing shortage of appropriately skilled resources, basic business considerations do not favor maintaining the status quo. In addition, industries in many nations worldwide are facing increased economic and regulatory pressures to establish a holistic approach to managing safety, traceability, cybersecurity, access control, and confidentiality procedures. For example, high-priority, prescriptive compliance frameworks from the North American Electricity Reliability Corporation (NERC) and the Federal Energy Regulatory Commission (FERC) require IT and operations staff in critical infrastructure to collaborate and manage risks cooperatively, and share relevant documentation to ensure security and reliability. Similar regulatory requirements have been called for in numerous other infrastructure areas, and the growing acknowledgement that IT underlies a great deal of these is leading to evaluation of what information systems should be among them. The European nations, with more trans-national infrastructures than those in North America, have pioneered this concept in published guidance[1], but it is gaining ground in other regions.

The operations of a multitude of industries, particularly those involved in energy production, transmission and distribution, large-scale manufacturing, transportation of people and materials, and all forms of automated processing, have become critically dependent on digital communications and computer networking abilities. Increasing connectivity of wired and wireless communications between growing numbers of intelligent devices has information technology appearing throughout the operational space by way of devices such as smart meters, automated asset distribution systems, and self-monitoring transformers. Products of this integration include the smart grid, smart manufacturing and processing plants, smart gas distribution, and smart water delivery. Many companies have addressed this technological dependency by building their own technology support teams within operational business units, often distinct and removed from enterprise IT (e.g. CIO). This creates duplications of staff, training and resources, as well as competing agendas and broken communications, all of which are prime targets for improvement. Organizational gaps can also raise governance, risk management and compliance issues of a nature to which engineering-oriented OT is unaccustomed. IT personnel have a longer history of information security and protection audits, and they can bring this to bear in collaborative efforts.

In 2012, interviews of 68 utility decision-makers at 39 North American utilities found that most said they consider improving their current level of IT-OT integration a higher-priority than planning for smart grid initiatives.

OT infrastructure assets are often widely distributed, requiring those responsible for its operation, support and upgrades to manually carry out their work in the field. However, advances in mobile access and computing provide field workers the ability to remotely access operational data

1 https://www.enisa.europa.eu/media/files/lock.jpg/view

and analysis tools, reducing the need for human resources to travel for equipment inspection, systems design, damage assessment and inventory monitoring.

Field automation devices, however, represent only one component in the growing Internet of Things[2]. Developments in recent history show that the benefits of IT-OT convergence are both diverse and extensive. The power industry, for example, has made substantial investments in the past decade to align these key business elements to improve business processes, increase electric systems performance, and ultimately improve customer satisfaction by reducing service interruption frequency and durations. The greater IT-OT convergence, taking place across many industries, providing intelligence to and communication with the lowest levels of distributed infrastructure, is increasing companies' ability to proactively manage their resources, optimize their systems and provide more effective workforces with greater insight and actionable information.

Integration promises numerous benefits, including:

- Improved automation, sensing and visibility
- Increased control over distributed operations
- Better compliance with regulatory requirements and tracking
- More responsive systems and improved organizational performance
- More effective workforce working with improved information
- Better strategic decisions based on more timely and accurate information
- Improved customer satisfaction resulting from increased proactive maintenance and reduced response times to unforeseen disruptions
- Improved stakeholder satisfaction resulting from improved flow of information

It must also be noted that the use of IP-based technologies in OT is well advanced already, and the change beyond the capability of any single entity or group to halt or redirect. The trend is ongoing, and any OT-dependent enterprise which resists adapting would eventually find itself without suppliers of or support for outdated hardware and software.

2 The Internet of Things (IoT) is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment.

3 CHALLENGES

With all of the advantages of bringing IT and OT together, the question becomes why convergence is not already the norm. The answers are numerous and somewhat contentious, but most considerations fall into a small number of categories stemming largely from their disparate history.

Technical

i. Environmental

Information Technology devices are chiefly placed in office spaces or enterprise data centers that are clean and temperature- and humidity-controlled, with either failover systems and/or local support staff available to respond quickly to performance issues, or both.

IT has rapidly developed around the needs for faster and more reliable data processing within the business sector. Increases in storage capacity, data transfer speeds, fault-tolerant architectures and protocols have transformed organizations around the world within the span of a few decades. Processing power has held to a rate of approximately doubling every 18 months for nearly 50 years, putting more power in one hand-held device than the entire U.S. National Space Agency had in the 1960s.

Operational Technology has evolved with a different set of priorities and resides in vastly different environments, often subject to extremes in pressure, humidity, and temperature. OT systems are distributed across wide geographical distances, with the expectation to function flawlessly without human support or intervention for years, or even decades. While enterprise computers are largely considered obsolete within two to five years, operational equipment is expected to be in place a minimum of 10-20 even in harsh manufacturing, refining and outdoor settings. It is not uncommon to find legacy equipment as much as 50 years old, still in place and functioning.

OT devices are designed to perform a very limited number of functions, often only one, according to exceedingly high reliability metrics. For example, a temperature-monitoring sensor in a boiler may not be improved by installation of high-speed processor, but the unfailing performance of its one duty, to consistently and accurately report the temperature, is an essential link in the chain that keeps the boiler from overheating and exploding. Understanding this distinction, that reliability and integrity are absolutely the primary considerations, is key to comprehending the divide between OT and IT, whether we are discussing their cultures, their organizations, or their technologies, as we are currently.

There's an oft-referenced bit of "knowledge" that allegedly states the percentage of office workers surveyed who wouldn't mind having to reboot their PCs a number of times per day just so long as it runs fast enough when in use. However large or small this number would be if we attempted to verify it, the corresponding percentage of operational staff willing to restart their systems would be zero. In most of these environments, it's all about the uptime.

ii. Compatibility

The establishment of broad international computing and networking standards has

enabled entire industries of hardware and software providers to continually create and update widely interoperable information-processing technologies. IT's rapid rate of innovation is one factor in the high value it places on error-checking, fault-tolerance, and failover capabilities. Compatibility is the intent, but it is understood that this is not 100% achievable in all situations, so preparedness for unintended buffer overflow or mismatched credential exchange is considered a basic cost of doing business.

OT is designed to function within exacting communication parameters, and many tools created to work in a business network cannot be used in an operational space without crashing systems. Network scanners, for example, generate traffic for which automation systems are unprepared, often disrupting normal operational communications and even causing device failure. The developers and vendors of computer network security products often lack the prerequisite knowledge of control systems requirements and limitations. Their software was developed for office environments and, until recently, with little consideration for the unique potential security concerns of control systems. OT depends on third-party vendors for much of its functionality, including device code, server applications and protocol stacks. OT vendor products are held to tightly defined requirements, but meeting these specifications requires positive performance testing, i.e. successful functioning under normal operational conditions . Introduction of unforeseen conditions yields unpredictable results, including unplanned forced shut down of critical devices, corruption of reporting and control data, and process disruption.

The effort needed to resolve these conflicts is often underestimated and far from inconsequential. OT equipment procurement practices include both a successful Factory Acceptance Test (FAT), to confirm devices meet the client tests and specification and is ready for installation, and a Site Acceptance Test (SAT), to confirm devices meet client tests and specifications after installation in their unique working environment. The SAT effectively transfers responsibility for equipment operations to the purchaser. Changes made after the SAT introduce risks, increases the complexity of vendor support and, in many cases, invalidate contractual warranties.

> **Cylance warned that attacks could "affect airline passenger safety". They found that hackers had almost ubiquitous access to systems at the compromised airports.**
>
> **- Fox-Brewster**

iii. Skills Shortage

Due primarily to the driving need for reliability, OT is the classic late adopter, often taking on new technology only once it has matured and any bugs have been addressed. This means that equipment in operating plants is generally older than those used in enterprises, and this leads to the need for its own skill set. While IT is driven by performance and security pressures to keep up with advancing technology, OT is driven by stability and interoperability demands to use and maintain systems at least a generation further behind. Windows XP, for example, which ended mainstream support in 2009 and extended support in 2014, can still be found in many operational networks.

An analogous dichotomy also exists

between the IT and OT workforces. IT professionals pursue career success and advancement through continually learning the latest technologies within operating systems, coding languages and applications. Labor cost management counts on a steady flow of new entrants, skilled in the most up-to-date tools and eager for employment. The need for workers familiar with older technology decreases as those systems and applications are obsolesced, and new workers with current skills generally lack experience with technology in use before they entered the workforce.

OT, with its mandate for caution, continues to use technologies long after corporate IT has abandoned them for faster, more secure, and more capable replacements. Skills considered outdated in IT remain in demand for far longer in OT environments, and the need for knowledge of the newest systems and applications is significantly lower and more delayed. New workers generally lack experience with technology in place before they entered the workforce, so the resources available for managing traditional OT systems are declining.

Workforce age also plays a role in the skills equation, as IT workers are younger, on average, than their counterparts in the OT space. The age gap is partly a result of IT becoming essential to business operations only relatively recently, and partly because it enjoys a strong and continuous stream of newly-minted college graduates eager to start their careers. Operations, perceived as an older and more stable profession, is seen as one with less opportunity where advancement or even entry may require post-graduate training and certification. As a result, IT has greater social allure for the young and ambitious. This is despite increasing demand for personnel in OT, with the oil and gas industry growth over the past decades, and roughly half of the energy sector workforce at or reaching retirement age this decade.

Further, OT workers come to their field through engineering backgrounds, with education and training in disciplines such as civil, electrical, or industrial and manufacturing. They will have recognizable similarities in how they approach accomplishing projects and solving problems. On the other hand, few IT workers have learned a traditional engineering perspective, although many bear certifications which include "engineer." The language shared between a mechanical and an automotive engineer is not spoken by the software or network engineer.

The different skills and language between IT and OT contributes to the communications and planning difficulties of converging these two highly technical business units. A common understanding of all the technologies involved must be established as a prerequisite to creating the blueprint of their future. Training and certification opportunities are increasingly available to address this need[3], and companies in the OT space are increasingly demanding qualified personnel, whether grown internally or through their hiring practices.

iv. Security

Just as the limited availability of radio technology skills and hardware once provided a degree of security to radio-controlled devices, only to evaporate with the commoditization of radios transceivers, so too did the protection afforded operational technology prior to the 1990s disappear. OT historically focused on physical security concerns, and correctly so. With systems generally operated by manual or proprietary electronic controls, they did not have the same risk exposures faced by their colleagues in IT. The majority

3 For example:
http://www.giac.org/certification/global-industrial-cyber-security-professional-gicsp
https://www.isa.org/templates/two-column.aspx?pageid=121797

of vulnerabilities required physical access or at least proximity to exploit, and security expenditures targeted controlling that access. Guards, cameras, fences, and locks; the usual suspects of secure facilities everywhere.

The increasing pervasiveness of connectivity has expanded the attack surface[4] of OT networks by opening them up to those dangers well known by information technology practitioners, and can only be expected to continue to do so. Every device accessible over electronic networks creates another point of attack for malicious operators; every additional connection between information and control networks multiplies the number of attack points that can be addressed. For example, building automation systems, rife with networked monitoring, control and reporting devices can be interrupted either by attacking the devices individually or disrupting the network itself, and automated pharmaceutical production can be halted by events as simple to implement as buffer overflow or denial of service attacks.

These ongoing developments, having long fueled the arguments for keeping these two disciplines distinct, must now be considered in light of means to address the concerns they raise. The relative maturity of IT in terms of network security does not translate directly to an ability to prevent or resolve these matters in the operational world. For all of the reasons discussed in this paper, OT security requires development of new tools and skills, drawing upon IT learning where applicable but maintaining a distinct awareness of the unique distinctions of this environment.

Organizational

Operational Technology and Information Technology have developed largely independently of each other, and their organizations and cultures reflect this divide.

i. Business Silos

IT builds, operates and maintains the systems on which modern businesses depend, including asset management, workflow management, geographic information systems, CIS/billing, and a host of other areas. Generally owned by the Chief Information Officer (CIO) or the Chief Technology Officer (CTO), IT may support information technology resources owned by operational business units, but the two divisions are not integrated, and IT-owned staff is directed by and answer to the IT hierarchy.

OT owns and operates devices controlling automated processes such as manufacturing or generation and distribution systems, and interfaces between these devices and the control room applications used to monitor and operate them. Leadership titles in OT include Chief Generation and Strategy Officer, Executive Vice President of Gas/Electric Operations, and Executive Vice President of Utilities. The OT organization may have staff trained to maintain the important IT systems it uses, but these IT-skilled individuals are OT resources and report to its management.

Ownership of the technology and management of the people touches on an aspect of integration seldom spoken of in positive terms: the reorganization. Reorganizing IT and OT divisions would

4 Attack surface refers to the sum of vulnerability exposures, all the points at which an attack could take place. SANS has a good explanation of it here: http://www.sans.edu/research/security-laboratory/article/did-attack-surface

potentially require deconstruction and validation of budgets, evaluation and justification of employee headcounts, restructuring of supervision-and-report charts, as well as many other labors required to 'get things right.' Stable and functional business processes will need to be adapted, retired or replaced; turf wars will have to end amicably or by force majeure, and fiefdoms will be broken apart.

How difficult these changes are for any particular enterprise will certainly depend on its leadership and quality of communications, but also heavily on its corporate culture. Smaller, newer, and more flexible companies often have measurably less resistance to change and may progress through reorganization efforts easily relative to larger corporations.

ii. Culture Clash

IT departments are often cost centers, supporting client business units within the larger enterprise. Some may establish their own policies and rules, particularly within the area of security, but their goals are largely established by the needs of others. They are fully staffed only during primary or extended business hours, as determined by their service agreements, with skeleton crews available to monitor systems during off-peak times. Planned outages are taken as needed and unplanned outages are responded to in accordance with the severity of the resulting disruption to business operations.

OT, in most cases, is core business. Staffing reflects the 24x7 nature of critical infrastructure. Planned outages are seldom, with systems expected to run for years, unassisted and without interruption. Unplanned outages, however, are crises that initiate emergency procedures and responses to restore normal operations.

Supervisory control systems, considered the heart of OT, originated over 60 years ago from the need to operate equipment located in remote locations, initially built by running device-specific wires between sites. OT personnel are engineers in the traditional sense, building and maintaining turbines and transformers (and, some argue, by temperament). They evaluate their work against a zero-faults expectation. Systemic changes are planned and practiced in advance, perhaps multiple times, to bring any potential for unforeseen events as close to zero as possible. A controlled shutdown is preferable to the risk of an OT system crash which may put lives on the line, as well as equipment and facilities ranging into the tens or even hundreds of millions of dollars to replace.

OT and IT place different emphasis on avoiding failures because the impacts of disruption are so radically different to each.

> "Cultural transformation is equally important as technical transformation in the move from the connected enterprise to the intelligent enterprise as significant organizational changes will be required to ensure successful outcomes. [It] begins by ensuring that not only do senior management support the strategy but are consistently talking about it as part of their regular company communications. Following on from this, the use of the Big Strategy needs to become part of how people undertake their daily roles."
>
> -Michael Sing, Schneider

> Advances have been made in developing a prototype universal transformer, including "a successful exercise that included the transporation, installation, assembly, commissioning and energization of the transformer ***in less than one week***."
>
> - DOE, Office of Electricity Delivery and Energy Reliability

Lost data can be restored from back-ups or recreated, lost power or product cannot, nor can human injury or death be undone. Communications lines for voice, data, or both, are increasingly often implemented with full redundancy, but production equipment less often. Over the past two decades, the failure of a hard drive in a high-utility server has decreased to little more than moments of labor to replace it. In fact, drive mirroring, RAID arrays and, more recently, virtualization of drives and servers have greatly reduced the impact of these events. Even a lost physical server can be restored in a few hours, and the advent of virtual server farms and cloud computing are making even that concept archaic. A downed transformer in a power grid, on the other hand, is little less serious now than it ever was. The failure of one can cause a cascade of others to fail and, even limiting the discussion to a single device, risk of injury or death is involved in its removal and replacement. Further, the time to resolve the problem is measureable not in seconds to minutes but in hours to months, depending on the size of the transformer, its location and whether a new one must be manufactured to custom specifications.

Some decades after the start of OT, depending on whether we consider the history of IT to begin with the isolated giants such as ENIAC in the 1950s or networked computers such as the ARPANET in the 1970s, Information Technology was born. Computer designers and handlers were initially at large research schools such as the University of Pennsylvania and the University of Illinois and, although IBM brought its engineering acumen to bear on its microcomputer, mold-breakers like Steve Jobs and Bill Gates most influenced IT growth and development. The U.S. Department of Defense's Defense Advanced Research Projects Agency (DARPA) funded the creation of the Internet's predecessor, the ARPANet, as a resilient, high-speed communications platform connecting scores of research universities. However, it was through the Usenet that countless numbers of college students and the general public became active users and contributors to computer networking.

Looking at the technological underpinnings and the populations involved, these are not divergent histories so much as parallel. IT was largely developed to address the needs and interests of the many: sharing, storing, analyzing and manipulating data. Just as IT systems are prized for flexibility and speed, so too are its human resources. The culture of operations, in contrast, values reliability and predictability over all other traits. Although many companies have introduced the two to each other in limited engagements over the past decade, the arrangement of a successful union requires careful consideration of both perspectives. This may be a shotgun wedding, but no one wants a trigger pulled.

iii. Risk Tolerances

In settings such as the financial industry, IT sits near the head of the table. Loss of data confidentiality impacts corporate reputations, loss of data integrity requires

expensive recovery procedures, and loss of data or system availability directly cuts off the flow of money. In other industries, the urgency placed on continuous availability lessens in accordance with the business' dependency on uninterrupted flow of accurate information.

OT performance directly impacts the corporate bottom line. Moreover, disruptions and outages have the potential to result in large-scale impact far beyond the enterprise and outside of the merely economic. The results of a power outage affects not only the lives of workers supporting and repairing failed power equipment, for there is an irreducible measure of risk involved in working with high-voltage equipment, but also the lives of those affected by the loss of power itself. While deaths directly attributable to power outages have historically been considered only those resulting from the shutdown of life support systems and heating/air-conditioning equipment, research has found that deaths from multiple causes rise when the lights go out. Outlier events like the blackout of 2003 are quite rare, but have enormous impacts, and operational personnel are trained to recognize their role in prevention.

Even restricting the discussion to potential effects of operational disruptions on corporate finances, losses are far from insignificant. The oil and gas industry routinely spends millions of dollars on seemingly small incidents such as a pipeline sensor failure when it causes undetected fuel leaks, and legal costs for power companies extend into that range each time a person is fatally electrocuted by their equipment.

The advent of electricity trading around the turn of the century created profits for many energy companies, but also increased their obligations. Regional transmission organizations (RTOs) operate the competitive wholesale markets, and their member companies' ability to sell their electricity is influenced by their reliability and capacity. Companies that don't meet their load or generation commitments must pay for that failure in amounts determined by the shortfall.

With the aversion to risk encouraged by these considerations, it should come as no surprise that operational personnel must carefully weigh many changes that IT considers part of daily routine. Network scanning, patching desktop and server operating systems, and installing firewalls and anti-virus software, are not only considered low risk in IT, but necessary to minimize risks of malware infection, data theft, and malicious attacks on information resources. OT, on the other hand, views these same processes as potential causes of downtime. Their perspective is informed by historical evidence, because these common IT tools have been repeatedly shown to crash OT systems.

> "During the [August 2003] blackout, mortality increased for accidental deaths (122% [95% confidence interval = 28% - 287%]), resulting in approximately 90 excess deaths" in New York City, the area studied.
>
> -Anderson and Bell

4 SOLUTION

Unfortunately, there is no simple way to overcome the technical and organizational challenges of an IT-OT convergence. The diversity in size, scope, structure and skill are too great for a comprehensive plan that is applicable to all organizational settings. Each enterprise must determine its own appropriate strategic plan and execute accordingly. Although there is not a universal convergence plan, there are considerations that must be addressed by any party intending to implement an IT-OT alignment strategy.

Leadership

The harmonizing of two such crucial units within the enterprise must take place with support and direction from the Chief Executive and the board of directors. No other entity has sufficient institutional standing or command of resources to take the charge and, even in the best of situations; conflicts shall arise irresolvable by those directly involved with the matters at hand. Sponsorship by the CEO can provide the necessary support, arbitration, and shield from external pressures generated by an undertaking of this scope.

Furthermore, for publicly held companies, the shareholders have to be considered. Even the most prepared firm will face some increases in expenditures, and the cost-benefit analysis of a convergence must be solidly conducted and thoroughly communicated. It should be very clear that resisting change in the near-term, might very well only lead to increased costs, both operational and transitional, in the mid- to long-term.

Planning

Accomplishment requires intent, coordination requires shared intent, and shared intent requires a plan. The integration of IT and OT can be a monumental project with staggering, possibly fatal, consequences of failure, risking both human lives and corporate survival. The alignment of all forces bearing on this task cannot be accomplished without a common plan to which they all subscribe. The plan must serve as the repository from which all parties refer and contribute as needed.

The planning phase, measured in length of time, may well exceed the implementation phase, and this is in accordance with best practice recommendations for large-scale projects. Flawed assumptions and errors found in planning have minimal impact relative to those found during implementation. Discoveries made during the formulation of a plan are invaluable in reduction or prevention of costs, and the establishment of interdepartmental communication protocols lays critical foundations for subsequent collaboration.

The organization as a whole and the integration team as a unit are both led from the top, but a plan is largely carried out at the bottom of the organizational chart. Knowledge of technical capabilities and limitations is most heavily concentrated among those who work with it regularly, the Subject Matter Experts (SMEs). Any plan that fails to invite and incorporate the SMEs' input is one that leaves potentially high-impact information to be uncovered at a later, and more expensive, time. Therefore,

organizations must ensure that the solid underpinnings of a plan include SMEs early in its development.
The enemy of every plan is reality, and it is a powerful foe. In addition to including the necessary resources, organizations must prepare for the unexpected. Successful planners not only prioritize minimizing risks before beginning implementation, they also anticipate the appearance of unforeseen events requiring corrective action. Their designs include flexibility and update cycles to iterate the plan and its components as needed. Oversight and control take place at not only the project level, but at multiple defined change-management and approval tiers beneath it.

Testing

It is an unfortunate reality that the generations of updates and upgrades to OT technology has left many parts untouched, uninvestigated and, in some cases, incompletely understood. While the maxim of 'don't fix what isn't broken' has a solid home in Operational systems, update and replacement cycles are growing shorter. Similar to mechanical equipment, OT needs to be maintained. Even the most knowledgeable of SMEs has some areas of uncertainty when it comes to predicting the behavior of OT equipment when exposed to changes, and the risks of introducing new technology to live systems and devices has already been discussed. As a result, some amount of pre-implementation testing, as determined by the organizational level of risk tolerance, is required.
Efficiencies may be found by identifying environments sufficiently similar for test results to apply across. In addition, a standard testing methodology utilizing simulations and/or offline, sandboxed equipment will greatly assist in streamlining both the testing process and in communicating the knowledge that comes from it.

Education

CIOs and CTOs often reference a lack of understanding between IT and OT as a major constraint on integration, as well as a shortage of sufficient staff with expertise in handling the technologies. Increased staffing budgets and targeted recruitment might help address one of these issues, but the best solution is to adapt the existing human resources by building the team to include both traditional and modern technical skill sets.

An educated workforce is crucial to success, and the education program in integration must address two distinct needs. First, the staff must embrace integration not only because leadership directs them to, but also because they understand the motivating forces behind the directive. This will be a cultural shift of the highest order for some, and changing an enterprise's culture is a tremendous challenge. Education is key to effecting that change.

Just as no individual can carry the entire plan in their head, no group has all of the training and experience needed to clear every technical hurdle potentially encountered in an IT-OT integration effort. Cross-training between the IT and OT departments will significantly reduce missteps and miscommunication. This is not to suggest a massive retraining program to teach network server administrators how to operate industrial smelters, but to develop an understanding of how their technologies differ, why their approaches may appear in conflict, and what each considers success. The technical specifics of the other party's duties may not be necessary, but a common ground for clear communications and collaboration is. Each organization needs to appreciate the knowledge, skills, and demands of the other. Fortunately, the availability of training and education tailored to fill this need is growing.

Observation

Changes of this magnitude are measured in years. Managers must keep track of milestones reached and deviations from original plans, as well as the evolving goals and scope of the plans. The definition of success established during the initiation and planning phases may not survive implementation. For example, the means to accomplish some objectives may be discovered unworkable or sub-optimal. Perhaps the original goal was a full integration of the two departments, and recent discoveries suggest the need for a third, inter-departmental group, or technological advances might outpace plans, making some intended work redundant. Regardless of the specifics, it is critical to keep the feedback loops open, to continue observing and evaluating the process and learn from ongoing efforts and developments impacting the overall project.

5 CONCLUSION

Operational and information technologies were developed to accomplish two distinctly different missions, with contrasting agendas and dissimilar tools and priorities. Decades of parallel development have provided each with unrelated processes and technologies running on distinct infrastructure, following separate standards, and managed by isolated organizational departments. Originating as discrete disciplines, their Venn diagram has incrementally grown to show a large area of overlap as OT has adopted IT-based technologies. Successful integration of these distant counterparts promises significant advantages in many areas, notably in performance and flexibility improvements, increased customer satisfaction, greater effectiveness of decision-making and business processes, and reductions in risks and costs.

There is no single way to win this race, however. This race is a long course requiring diverse skill sets to overcome the numerous obstacles on the way and a high cost to any missteps. One clear precursor to getting started is a mapping of the current and future zones of responsibility and the unique route the organization will travel between the former and the latter. Along the way the enterprise must coordinate IT and OT to implement a centralized management of security, create shared governance models and common business and operational processes, and cross-train employees to build a team of resources familiar with both disciplines.

This coordination requires a strong, disciplined project and change management supported by the highest levels of business. Executive leadership must define and communicate the organizational vision in order to overcome internal conflicts and maintain focus on the universal benefits of integration. Management must find and allocate the resources demanded for accomplishment of this major organizational effort.

Organizations that dedicate themselves to overcoming the divisions between the disparate OT and IT units will gain a significant competitive lead over their peers who do not. Both lines of business will discover currently unrecognized potentials as they learn to increase interoperability, refine processes, and develop collaborative decision-making in support of common objectives. While certainly a challenging and laborious undertaking, the long-term benefits of IT-OT convergence are well worth the effort.

This paper draws many of its examples from the energy, oil & gas, and financial industries, as these are widely considered the most vulnerable and disruptions of their operations to have the greatest and most immediate national impacts. The difficulties discussed and the recommendations made are equally applicable to all industries using OT.

Bibliography

Lucas Apa and Carlos Mario Penagos, (2013). "Compromising Industrial Facilities from 40 Miles Away." Presented at Black Hat USA 2013. https://media.blackhat.com/us-13/US-13-Apa-Compromising-Industrial-Facilities-From-40-Miles-Away-Slides.pdf

Michael Assante, President and CEO National Board of Information Security Examiners of the United States Inc., "Securing Critical Infrastructure in the Age of STUXNET," Testimony to the Senate Committee on Homeland Security and Governmental Affairs, U.S. Senate, November 17, 2010, 3, http://www.hsgac.senate.gov/download/2010-11-17-assante-testimony.

G. Brooke Anderson and Michelle L. Bell, "Lights out: Impact of the August 2003 power outage on mortality in New York, NY"
http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3276729/

Infrastructure Security and Energy Restoration Office of Electricity Delivery and Energy Reliability, U.S. Department of Energy. "Large Power Transformers and the U.S. Electric Grid" (April 2014 Update)
http://tdworld.com/site-files/tdworld.com/files/uploads/2014/05/LPTStudyUpdate-040914.pdf

Michael Sing, "IT / OT Convergence Part 3 – On the way: moving to the intelligent enterprise"
http://blog.schneider-electric.com/machine-and-process-management/2013/11/18/ot-convergence-part-3-way-moving-intelligent-enterprise/

ISO New England Inc., Overview of New England's Wholesale Electricity Markets and Market Oversight, 2013.
http://www.iso-ne.com/pubs/spcl_rpts/2013/markets_overview_051513_final.pdf

HÄmmerli, Bernhard, and Andrea Renda,

PROTECTING CRITICAL INFRASTRUCTURE IN THE EU: CEPS TASK FORCE REPORT
http://aei.pitt.edu/15445/1/Critical_Infrastructure_Protection_Final_A4.pdf

"in March 2007 an experiment (the Aurora Generator Test) conducted by the Idaho National Labs in the US demonstrated that a large diesel generator could be severely damaged by exploiting a computer vulnerability, revealing that physical damage could be done through the computer system."

For Further Reading:

www.Nexdefense.com/ICS_Lexicon

www.Nexdefense.com

APPENDIX A: Selected OT Disruption Incidents

The following comes from the US Office of Government Accountability Report:

http://www.gao.gov/new.items/d071036.pdf

CSX train signaling system: In August 2003, the Sobig computer virus was blamed for shutting down train signaling systems throughout the East Coast of the United States. The virus infected the computer system at CSX Corporation's Jacksonville, Florida, headquarters, shutting down signaling, dispatching, and other systems. According to an Amtrak spokesman, 10Amtrak trains were affected. Train service was either shut down or delayed up to6 hours.

Taum Sauk Water Storage Dam failure: In December 2005, the Taum Sauk Water Storage Dam, approximately100 miles south of St. Louis, Missouri, suffered a catastrophic failure, releasing a billion gallons of water. According to the dam's operator, the incident may have occurred because the gauges at the dam read differently than the gauges at the dam's remote monitoring station.

Bellingham, Washington, gasoline pipeline failure: In June 1999, 237,000gallons of gasoline leaked from a 16-inchpipelineand ignited an hour and a half later, causing three deaths, eight injuries, and extensive property damage. The pipeline failure was exacerbated by poorly performing control systems that limited the ability of the pipeline controllers to see and react to the situation.

Zotob worm: In August 2005, a round of Internet worm infections knocked 13 of Daimler Chrysler's U.S. automobile manufacturing plants offline for almost an hour, leaving workers idle as infected Microsoft Windows systems were patched. Zotob and its variations also caused computer outages at heavy-equipment maker Caterpillar Inc., aircraft maker Boeing, and several large U.S. news organizations.

APPENDIX B: Terms and Definitions

Building management/Automation System (BAS): an electrical system controlling a facility's heating, ventilation and air conditioning (HVAC) system. May also control lighting, fire safety and security systems, plumbing, elevators, etc. Generally architected as a Distributed Control System.

Distributed Control System (DCS): a control system comprised of control elements distributed throughout a facility such as a refinery, power or manufacturing plant, mine, network of pipelines, or ship. Generally consists of a number of supervisory computers and one or more controlling computers in a hierarchical arrangement. It may also include coordinating computers between the supervisory and control levels.

Historian: a software service within an industrial control system which accumulates time-stamped sensor and event data in a database which can be queried or used to visualize trends in the Human-Machine Interface. The historian is a client that requests data from a data acquisition server.

Human-Machine Interface (HMI): a computer enabling a human operator to monitor and interact with control systems and processes. It analyzes and presents data requested from sensors and data acquisition servers.

Industrial Control System (ICS): an umbrella term used to refer to multiple types of control systems, including Distributed Control Systems, Building Automation Systems, Programmable Logic Controllers and Supervisory Control And Data Acquisition systems. A similar term, Process Control Domain (PCD), is common in the Oil & Gas industries.

Industrial Internet: the interconnected web of intelligent industrial products, services and processes that communicate with people and each other.
Industrial Internet of Things (IoT): the next evolutionary phase of OT, in which operational technology extends functions and capabilities through the Industrial Internet. This is an ongoing development.

Operational Technology (OT): the hardware and software automation and control systems and components that monitor, measure, and protect infrastructure ranging from fleets of machines to power grids, refineries, and manufacturing and processing plants. It monitors and/or controls physical equipment and events.

Process Control Network (PCN): a communication network providing communication of data and commands between monitoring, measuring and control components of a SCADA system.

Programmable Logic Controller (PLC): a computer used to automate industrial equipment or processes. Largely applied to limited-purpose and hardened devices designed specifically to operate in industrial working environments.

Remote Terminal Unit (RTU): co-located with sensing equipment to collect and communicate data to supervisory systems in a SCADA network, as well as to receive supervisory commands and communicate to the connected equipment. Often have limited control capabilities.

Safety Instrumented Systems (SIS): control systems specifically engineered to fail to a "safe" state to reduce the likelihood or prevent safety, health and environmental impacts.

Supervisory Control And Data Acquisition (SCADA): a system, which monitors, reports on and controls remote equipment. Generally consists of one or more supervisory and control computers, data acquisition computers, programmable logic controllers, remote terminal units, one or more historians, and a Process Control Network.

Contributors

The authors would like to thank the following people for their supportive contributions:

Doug Wylie

Graham Speake

Jamey W. Sample

Michael J. Assante

Author Bios

Derek Harp: Co-Founder and Executive Chairman of NexDefense

A serial entrepreneur and pre-seed investor in technology companies, Derek has founded, led, and advised new enterprises for more than 20 years. In addition to his current role with NexDefense, Derek helped launch and provides leadership to the Industrial Control Systems (ICS) Cybersecurity Business at the SANS Institute. He is also a founding steering committee member and co-manager of the Global Industrial Cyber Security Professional (GICSP) certification, which launched globally in 2013.

A Navy veteran, Derek served as a U.S. Navy Surface Warfare Officer tasked with physical security, combat information management, communications security and intelligence responsibilities.

After distinguished service in the Navy, Derek launched his career in the private sector as the Co-Founder and the CEO of LogiKeep, Inc., a network security intelligence firm. During his time with LogiKeep he co-invented Intellishield™, a pioneer IT security product later acquired by Cisco Systems. Under his leadership, LogiKeep experienced extremely rapid growth, serving dozens of Fortune 500 companies, including those in major financial and pharmaceutical distribution industries and government institutions.

Derek is a recognized thought leader, frequently appearing in national publications and speaking events on the topics of entrepreneurship, capitalization, business, intelligence systems and security.

Bengt Gregory-Brown: Principal Consultant at NexDefense

Mr. Gregory-Brown is the principal analyst at Sable Lion Ventures, LLC, a virtual accelerator focused on emerging cyber security solutions. He brings twenty years of experience in management of IT and infrastructure projects, enterprise security governance, information security risk analysis, regulatory compliance and policy conformance for companies including Liebert Systems, American Electric Power, Xerox and Nationwide.

Mr. Gregory-Brown was also a Co-Founder and director of LogiKeep, Inc., and instrumental in the crafting of its premier IT security product, Intellishield™. Additionally, he has managed IP development and protection strategies from executing ideation sessions through patent process administration, and is a co-inventor of multiple issued patents. Current clients include NexDefense, Inc. and the SANS Institute.

NEX DEFENSE

www.nexdefense.com

1.800.725.0814