Using Commercial Off-the-Shelf Mobile Devices in Industrial Automation:

"Russian Roulette" or the "New Normal"?

Introduction

At a stone quarry in Pennsylvania, two powerful 6-inch (15 cm) pumps remove millions of gallons of water that builds up from rainfall and runoff each year. An electrician standing at the quarry's edge pulls out his iPhone®, opens a web browser, and types in a URL and his password. On his screen he sees data for each pump—status and current draw—plus flow rate and the water level in the quarry. No problems, so no need to go down into the quarry. He moves on to his next task.

In California, control technicians at a citrus fruit processor adjust the speeds of conveyors routing fruit for washing and labeling. The noise level in the plant is high, and the HMI that controls conveyor speed is on the far side of the room. Instead of shouting to the operator at the HMI, the technician watching the fruit move through the equipment uses an app on his Android™ smartphone to fine-tune the conveyor.

The move to mobile

Increasingly, automation engineers and technicians are seeing the value of using commercial, off-the-shelf (COTS) mobile devices for situations like these:

- Remotely accessing equipment
- Commissioning and maintaining systems
- Providing inexpensive machine operator interfaces

But is this move to mobile a disaster waiting to happen or the future of automation?

Recent LinkedIn® discussions in automation groups show the wide divide between those who fear the new mobile technology and those who embrace it. A January 2014 discussion in the ISA - International Society of Automation group garnered typical comments on both sides:

"A breach in system security can destroy the safety system. It looks like Russian roulette."

"Think about what you could do if you had a 3D model of your plant on a tablet right in the field!"[1]

Who is right, and where do we go from here?

This paper takes a look at mobile trends in business and the pros and cons of using COTS mobile devices in industrial automation. The paper also gives practical advice for choosing mobile devices—whether off-the-shelf or not—suited to your automation application.

Mobile is personal

Most of us have quickly gravitated to smartphones and tablets in our personal lives, emailing and texting, playing games and reading, posting on Facebook and Twitter, watching videos and taking them, even banking and paying bills online.

It's easy, it's fast, and you can do just about anything you need or want to, anywhere in the world. Music, maps, a digital camera or two, notebook, address book, calendar, stopwatch, alarm clock, calculator, photo album, GPS, encyclopedic dictionary, complete retail stores—oh yes, and also a phone—all of these and more are in your pocket ready to use.

The younger you are, the less you realize how amazing this transformation is and the more you simply expect the incredible convenience of mobile, wherever you are.

1. LinkedIn ISA group discussion, January 2014, http://www.linkedin.com/groupItem?view=&gid=137598&type=member&item=5817404882721718275&qid=770a54eb-e4c3-4d07-be43-af00e7bfc7c8&trk=groups_items_see_more-0-b-ttl

So why should this convenience stop at the door to your workplace?

Increasingly, it doesn't.

Mobile means business

In 2009 Intel found employees bringing their personal mobile devices to work, and about two years later the company projected that by 2014, 70% of their employees would be using their own devices in their jobs.[2] Other companies noticed the same trend, dubbed "bring your own device" or BYOD.

"BYOD strategies are the most radical change to the economics and the culture of client computing in business in decades," noted David Willis of industry analyst Gartner in 2013. "The benefits of BYOD include creating new mobile workforce opportunities, increasing employee satisfaction, and reducing or avoiding costs."[3]

Employees have good reasons for wanting to use their mobile devices in business: these devices are easy to use, familiar, powerful, and offer capabilities not available through bulky computers or even laptops. Over the last five years, computer technologies have advanced so quickly for consumers—especially in mobile devices—that consumer computing began driving business computing for the first time.

"Employees routinely report to work with more computing power in the palm of their hand than their desktop machines held just a decade ago," noted Bill Lydon in a 2012 Automation.com column.[4]

New opportunities

The BYOD trend has been met with intense worry as well as great enthusiasm. Company and employee concerns about employees using their own devices at work are real: network security, privacy, who pays for the device's data plan, and so on. We all have our own ideas about whether employees' personal devices belong at work.

But no matter which side of the debate you stand on, the rapid growth of this trend shows us something important: the power of COTS mobile devices to make a difference in business. Mainstream smartphones and tablets create new opportunities to simplify our jobs and streamline our tasks, and we don't want to do without them.

What is COTS all about?

The concept of COTS didn't start with mobile devices. The term was popularized in the mid-1990s when then U.S. Secretary of Defense William Perry supported a major change to military purchasing guidelines.[5]

Instead of designing and building their own hardware and software, the military began looking first for technology and products that were designed and built by commercial firms and offered for sale to the general market—commercial off-the-shelf or COTS products.

COTS products are attractive for several reasons:

- **Cost.** Development costs have been spread out over a broad market, so the product is less expensive to buy.
- **Availability.** Products are readily available and can be quickly acquired or replaced. You don't need to wait months or years to get them, nor do you have to keep expensive spare parts in stock.

2. Mobile: Learn from Intel's CISO on Securing Employee-Owned Devices (webinar, not dated), http://www.govinfosecurity.com/webinars/mobile-learn-from-intels-ciso-on-securing-employee-owned-devices-w-264
3. Gartner press release May 2013, http://www.gartner.com/newsroom/id/2466615
4. Bill Lydon, "Is BYOD (bring your own device) worth the risk?" 17 Dec 2012, http://www.automation.com/automation-news/article/is-byod-bring-your-own-device-worth-the-risk
5. COTS Journal online (undated), http://www.cotsjournalonline.com/pages/about_us

- **Integration.** Because products in the general market are used by a wide range of businesses, common standards are often built in, making interoperability easier.
- **Capabilities.** Due to competitive pressures, more frequent product updates add new features and support for the latest technologies.
- **Associated costs.** Support and training costs are lower because the product is well known and familiar to technicians and employees.

Meanwhile, back at the factory...

These are the same reasons industrial automation experienced its own move to COTS hardware nearly 20 years ago, when PCs first began to infiltrate the factory floor. Off-the-shelf PCs are now an integral part of our industry and used in a variety of settings.

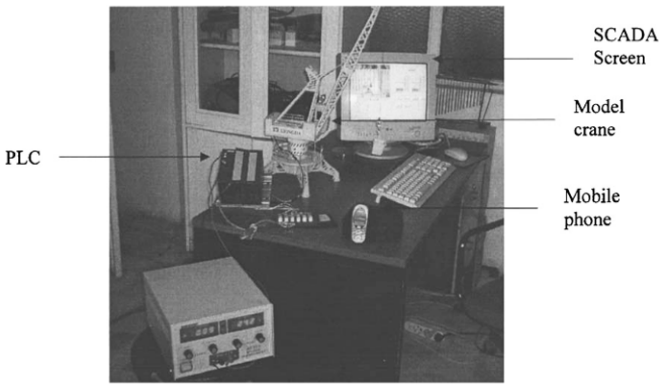
What we're seeing now appears to be the first wave of a similar off-the-shelf product adoption in mobile devices for automation. With the current speed of technological change, it probably won't take 20 years, or even 10, for mobile to become standard in the industry. But what are the concerns for automation companies?

For employees in offices, using email on a smartphone or opening PDF documents on a tablet is easy and convenient. Most business environments run on Ethernet networks and Internet standards such as TCP/IP; compatible Wi-Fi networks are easy to add, or employees can use cellular networks. And except for companies with highly sensitive data, like financial institutions and government agencies, mobile devices seem much more like an opportunity than a problem.

But industrial automation companies, with their proprietary buses and traditional interoperability bottlenecks, are less obviously suited to employees using off-the-shelf mobile devices.

Mobile adoption in automation has been slower than in other fields, though enthusiasm began early. In 2004 two researchers from Turkey theorized that mobility could make workers in industry more productive. Their proof of concept? They used a mobile phone to control a model crane using a SCADA system.[6]

It would take a few more years to see real-world adoption, but it's clearly here now. In December 2013, engineers



Early experiment using mobile in automation[6]

reported that they use a wide range of mobile apps and built-in mobile features in their jobs:

- Apps for flow calculation, conversion, simulation, and drawing
- Apps that show standards, for example for connectors or electrical wiring
- Built-in sensory tools for testing, like GPS, gyro, magnetic field, accelerometer, and proximity sensors
- Built-in cameras, for example when designing around existing equipment or troubleshooting with an OEM (original equipment manufacturer)
- Apps for monitoring and controlling PAC or PLC systems[7]

These responses came from engineers of all ages; but expectations from younger engineers are even greater. As they begin to enter the factory, they simply assume the same capabilities they grew up with will be present.

"'We see the younger employees of our customers walk up to an operator interface and try to manipulate the screen using the pinch and zoom movement with their fingers,' reports Tom Craven, OI/HMI product manager at GE Intelligent Platforms. 'When they realize they can't control

6. E. Ozdemir and M. Karacor, "Mobile phone based SCADA for industrial automation," ISA Transactions, V 45, No 1, Jan 2006, pp. 67–75, http://akademikpersonel.kocaeli.edu.tr/eozdemir/sci/eozdemir21.12.2009_11.48.34sci.pdf
7. LinkedIn Automation & Control Engineering group discussion, Dec 2013, http://www.linkedin.com/groups/What-engineering-related-mobile-apps-do-1967039.S.580645873421753958 8?qid=cbe791df-9f49-4d5b-9b13-e77ade69d734&goback=.gde_1967039_member_5832829489855352832.gmp_1967039

the screen and information that way, there's this reaction of *Why not?*"[8]

It's no wonder off-the-shelf smartphones and tablets are appealing.

- They're compact, lightweight, affordable, and readily available.
- They offer powerful processors and high-definition screens with multi-gesture touch.
- They have built-in wireless networking (IEEE 802.11) and security protocols (Wi-Fi Protected Access II, or WPA2),
- Lots of developers know how to program for them, so useful web-based and native apps are appearing quickly.
- And COTS mobile devices are familiar, especially to younger engineers, so training costs are much lower.

Industry 4.0 and friends

A raft of terms—the Fourth Industrial Revolution, M2M, the Internet of Things, Industrial Internet, Industry 4.0—all point to the growing interconnectedness of sensors, actuators, machines, and processes with each other and with the humans who work with them.

Hannover Messe in 2013 reflected a future vision that included improved interaction between machines and between machines and people, a merging of IT and automation, and a closer relationship between design and manufacturing.[9]

8. James R. Koelsch, "Time to upgrade your HMI?", *Automation World*, 8 March 2014. http://www.automationworld.com/control/time-upgrade-your-hmi
9. Suzanne Gill, "Industry prepares for the next industrial revolution," *Control Engineering*, 27 June 2013. http://www.controleng.com/single-article/industry-prepares-for-the-next-industrial-revolution/6a00860f7b0971e42ea1a9a7114468e4.html

If you don't provide your employees mobile apps...your competitors will be doing it...and hiring key talent away from you.

- Philippe Winthrop, Enterprise Mobility Foundation

While some of this future vision reduces human involvement, perhaps even more of it links humans and machines for more efficient design, monitoring, and control of sensors and systems.

Wireless network development and increasingly smaller and more powerful computers make this possible. Process industries such as water/wastewater and oil & gas have far-flung installations that cry out for remote monitoring. In factories, technicians can manage equipment in another room or in another part of the world.

"If you don't provide your employees mobile apps, you'll not only lose productivity (time to action), but you'll eventually have a harder time attracting new talent because the next generation workforce will be expecting this...and your competitors will be doing it...and hiring that key talent away from you," notes Philippe Winthrop of The Enterprise Mobility Foundation.[10] (23)

Considerations for using COTS mobile in automation

So mobile is part of our future in automation, and if you haven't thought much about it, now is a good time to start. When you're considering using mobile devices in industrial settings, you'll want to think about four factors: environment, safety, security, and connectivity. Let's take a closer look at each of these.

Environment

Industrial environments vary widely. Harsh environments can kill a mobile device. Drop an unprotected iPad® onto concrete and you've got a problem. Use a smartphone in extreme heat, severe cold, or over 95% humidity, and it won't last long. Water and chemicals corrode. Dust and dirt scratch and clog screens and buttons.

10. Philippe Winthrop, "Thinking About The ROI of Mobile Apps? Think Instead About Sports Advertising," 20 Dec 2013, blog post. http://theemf.org/2013/12/20/thinking-about-the-roi-of-mobile-apps-think-instead-about-sports-advertising/

If your environment is harsh, you may need to look at ruggedized devices. Mobile manufacturers like Panasonic® and DAP Technologies™, for example, have developed a variety of ruggedized tablets that meet military standards (such as the U.S. Department of Defense MIL-STD-810) and/or qualify for high IP (International Electrotechnical Commission Ingress Protection) ratings.

- MIL-STD-810 covers shock, vibration, altitude, humidity, extreme temperatures, dust, and several other conditions.
- IP ratings are usually two-digit numbers, the first number for dust (solids) and the second for water (liquids). For example, an IP rating of 65 means a device is dustproof and can protect against low-pressure water jets from any direction.

OtterBox Armor series case

But many industrial environments don't require this kind of protection. And ruggedized mobile devices are not only significantly more expensive, but also rarely match the features we appreciate and expect on our personal devices: multitasking, gestures beyond the basics, built-in sensors, voice recognition, cameras, communications through email and texting, and much more.

Personal devices are becoming more robust as well. Corning® Gorilla® Glass 3 is highly scratch, chemical, and break resistant and is the standard screen cover glass in many consumer mobile devices.

Hoffman iPad stand

Corning even has an antimicrobial cover glass. With toughness and optical clarity similar to regular Gorilla Glass, the company says it also reduces bacteria by more than 99.9%. Antimicrobial glass could be a good choice for a tablet, phone, or iPod used as an HMI on machines, kiosks, or walls, where many people touch it.[11]

11. Corning website, http://www.corninggorillaglass.com/Antimicrobial

Protective cases are now available to toughen off-the-shelf smartphones and tablets, too. An inexpensive OtterBox®—designed for personal use and available for a variety of brands and sizes—can protect against dirt and dust, a 10-foot (3 m) drop onto concrete, two tons (907 kg) of pressure, and immersion in 6.5 feet (2 m) of water for 30 minutes.[12]

Other solutions include low-cost field protection against water, dirt, and shock from LifeProof™, and iPad stands and enclosures from Hoffman®.[13]

Safety

Safety is a critical component for industrial settings. In locations with high concentrations of dust, or flammable liquids or gasses, *intrinsically safe* wireless devices—phones, calibrators, and other portable instruments—may be required. Intrinsically safe products limit current and voltage so that they cannot produce sufficient energy to cause a spark.

In less-hazardous areas, however, COTS mobile devices are not considered a problem. In the early 2000s a spate of reports in the press, later debunked, claimed to connect cellphone use to fuel station fires.

In response, the U.S. Federal Communications Commission wrote, "...while it may be theoretically possible for a spark from a cell phone battery to ignite gas vapor under very precise conditions, there is no documented incident where the use of a wireless phone was found to cause a fire or explosion at a gas station."[14]

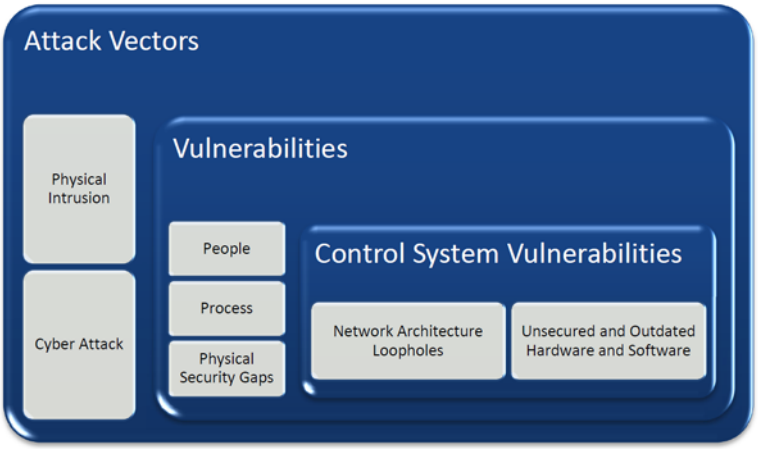
Scientific testing...has not established a dangerous link between wireless phones and fuel vapors.

- U.S. Federal Communications Commission (FCC) Consumer Bulletin, rev. 1-17-2013

12. OtterBox website: https://www.otterbox.com/
13. Reviewed by *Control Engineering*, http://www.controleng.com/single-article/commercial-tablets-get-industrial-enclosures/d689b9f8cf6d9298b5aa68caca026ffe.html
14. FCC Guide, "Wireless Devices at Gas Stations," https://www.fcc.gov/guides/wireless-phones-gas-stations

In some applications, protective equipment like helmets, goggles, and gloves can make it difficult to see a screen or handle a mobile device, whether ruggedized or COTS. Modern capacitive touchscreens rely on your body's ability to conduct electricity; cover your fingers in thick gloves and your swipes and taps won't work.

Another potential problem with protective gear is unintended gestures on the device. Whether stored in a padded pocket or inadvertently brushed with a glove, the industrial equivalent of "butt dialing" can be avoided simply by building verifications into the interface.



Source: Frost & Sullivan

But in the many areas where protective gear isn't needed, these concerns don't apply. More attention is being paid to the safety *advantages* of mobile: "You can keep cabinet doors closed and keep a safe distance away from the energized equipment," notes one engineer.[15]

Security

Security concerns for automation companies often go beyond the normal business concerns about company data, because critical processes and equipment are key in industrial control.

Proprietary control networks not connected to any other systems make security much easier than Ethernet or wireless networks, precisely because they are isolated and few people understand them. But closed, proprietary networks also lock useful data inside.

As Ethernet and especially wireless systems become more common in industry, and as connections between control systems and business systems become more common, this valuable data becomes useful in many ways.

- Supply chains become more efficient, with deliveries tied directly to current needs.
- Realtime production data informs management business decisions.
- Equipment status data drives maintenance, improving efficiency and reducing downtime.
- Systems and equipment in remote or hazardous areas are easily monitored and adjusted, reducing employee time and expense and increasing safety.

The benefits of making data available are obvious, but the importance of securing that data is obvious as well.

As their realms become interconnected, information technology (IT) and industrial automation (IA) personnel must work hand-in-hand to protect network security, and turf wars between IT and IA must give way to alliance against a common enemy.

Because IT already has experience with securing Ethernet networks, they can often help control engineers design network segments, purchase suitable routers, and install firewalls.

Control system security is just part of an overall security plan that includes far more than computer networks. Frost & Sullivan suggest:[16]

- Looking at all possible attack vectors, both cyber and physical
- Thinking about all your vulnerabilities: people, processes, and physical security gaps
- And then considering your control system vulnerabilities

Control system security levels

The best system security is multi-layered, starting with access to the mobile device itself, continuing to its communication with your company network, and ending

15. LinkedIn discussion in ISA - International Society of Automation group, Feb 2014. http://tinyurl.com/qda5qxs

16. Ivan Fernandez, "Cybersecurity for Industrial Automation & Control Environments," April 2013, http://www2.schneider-electric.com/documents/support/white-papers/white-paper-cybersecurity-for-industrial-automation-control.pdf

with layers of protection for the automation system and key pieces of equipment.

Device access. Manufacturers are experimenting with a variety of password protection methods for accessing COTS mobile devices: simple number locks, a pattern swipe (Android), a fingerprint scanner (iPhone), facial recognition (Android), a gesture-on-a-picture (Microsoft® Windows®). All of these methods can help keep unauthorized people from using the device.

If you supply devices to your employees, you may want to look into other protections as well, for example:

- Endpoint protection programs, similar to anti-malware and security applications on PCs
- Isolated virtual environments (also called *containers*) that separate personal apps and data from company apps and data on the device

Device communication. One advantage of COTS mobile devices is that security standards for communication are built in. When you check your bank balance or pay bills online from your phone, you use its built-in Wi-Fi Protected Access II (WPA2) security, a protocol called secure sockets layer (SSL), and some combination of username, password, and perhaps images or special questions to verify that you have the right to take those actions.

Similar standards must be used in your industrial mobile apps to verify users and track operator actions.

You may even want to look at mobile device management (MDM) client programs for mobile devices. These programs give your IT department the ability to control software, track a device's location, and regulate the use of company systems by anyone using the device.

Automation system protection. Whether you use COTS mobile devices or not, your company networks, both IT and automation, must be made as secure as possible. Mobile devices are only one part of an overall security strategy designed to identify, authenticate, and track users; control access; and monitor and respond to any unusual activity.

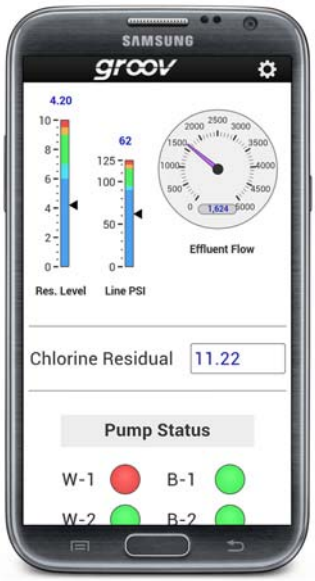
An August 2013 white paper from network device manufacturer Moxa suggests several actions to take:[17]

- Segment IA from the rest of the company.
- Segment subsystems and key equipment.
- Disable unused ports on networked devices.
- Filter incoming MAC addresses to allow access only to authorized devices.
- Use a deep packet inspection (DPI) firewall to identify suspicious use from authorized sources.
- Monitor passwords for strength, and force periodic change.
- Always change default usernames and passwords on networked devices.
- Use a virtual private network (VPN) for remote access.
- Train employees on safe Internet usage.

Data backups

If technicians use mobile devices to gather and store data, for example from remote equipment, another consideration is keeping that data safe and available if the device is lost or damaged.

Backing up data to the cloud or to a company server are options to consider, depending on the confidentiality of the data.



Connectivity

As the Internet of Things expands, adding wireless capability to an increasing number of sensors and equipment, COTS mobile devices become attractive for their ability to connect. With a variety of standard wireless options built in—cellular (3G, 4G, LTE), wireless LAN (Wi-Fi), and often Bluetooth—they simplify connections to your business and automation systems.

Of course your application and environment will determine whether wireless connectivity is a concern. In hazardous environments wireless devices may need explosion-proof certification. In addition, some industrial settings may find

17. Jim Toepper, "Industrial Networking Security Best Practices," 20 August 2013, http://www.logic-control.com/media/Moxa_security.pdf

wireless networking problematic due to signal interference from equipment and machinery.

In other industrial settings, wireless networks can work consistently well and provide a new method of connectivity that makes maintenance and monitoring easier.

The location of the systems and equipment you want to monitor and control affects how you connect to them. If you're commissioning a system or checking KPIs within your facility, for example, your mobile device will connect through your local wireless network. If you're monitoring production miles away or controlling remote pumps, you'll need to connect over the Internet.

Whenever you connect to a private company network over the Internet, most security experts recommend using a virtual private network, or VPN. The VPN creates a kind of protected tunnel through the Internet for increased security. COTS mobile devices have a VPN client built in, which simplifies setup for a VPN.

New tools for mobile interfaces

So perhaps you've decided that COTS smartphones or tablets could be useful in your application. Before you move ahead, there's one more thing to think about: the operator interface for your mobile device.

If someone else builds the app and you just download it, you have no control over what goes into it (although most app developers are interested in making their apps useful and may appreciate suggestions.)

But an increasing number of manufacturers are making tools available so you can create a mobile interface for your equipment or system, or adapt an HMI you already have. One of these is Opto 22's *groov*[18], a web-based tool for both developing and using mobile operator interfaces.

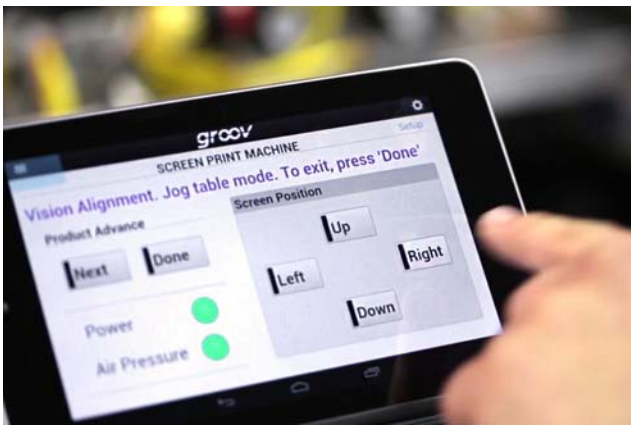
groov's premise is simplicity:

- Interfaces can be built on any brand computer with a modern web browser. No plugins are required.
- Interfaces are built quickly and require no programming or coding. The developer drags and drops indicators and controls from a built-in library of gadgets, then tags them from his existing database on a tag server.

Users must determine whether they want to get more from their machinery. For example, being able to see a video on how to repair a machine when a particular fault occurs can help to minimize unplanned downtime.

- Raul Guerrero, Eaton, quoted in *Automation World,* "Time to Upgrade Your HMI?" March 2014

- Interfaces for phones and tablets are built at the same time, but each can be modified to place gadgets where they are most useful.
- Interfaces can be built for almost any automation system, because *groov* acts as an OPC-UA client. Used with a communications platform like Kepware Technologies' KEPServerEx[19], *groov* can access a wide variety of control systems.
- Permissions are assigned to specific users based on the screens they need to see. Individual usernames and passwords are required to log in.
- Interfaces are served to authorized users from an industrially hardened *groov* Box or from a Windows PC acting as a server.
- All communications between devices and the *groov* server are encrypted for security using WPA2 and SSL.
- Because they are web based and use Internet standards, *groov* interfaces can be viewed on virtually any device with a modern web browser, regardless of its size or brand. Interface elements automatically scale to fit the size and shape of the device, while remaining large enough to see and use.



18. groov website: http://groov.com/

19. Kepware website: http://info.kepware.com/kepserverex-and-groov

Moving ahead

So what's the answer to our question, is mobile in automation "Russian roulette" or "the new normal"?

Possibly both. It depends on you.

COTS mobile devices are already being used in industrial automation, and the trend will accelerate. The only question is whether you'll be prepared.

Start thinking now about the environmental, safety, security, and connectivity factors your automation system requires.

Work with IT to build your security infrastructure and with management to establish mobile policies.

Decide whether you will provide mobile devices to employees. Decide whether employees' personal devices should be used for business purposes.

Make sure everyone understands the rules and reasons for how mobile devices (both personal and company-supplied) may be used in your facilities.

And start now to **think about how COTS smartphones and tablets can help your business** be more efficient and competitive. Talk with other engineers, technicians, and managers about specific ways mobile can be useful to you and your company.

"What's lacking is broad recognition of what has become possible, and the vision to utilize these new technologies to transform industry," says Andy Chatha of ARC Advisory Group.[20]

Our challenge as automation professionals is to embrace connected intelligence in an intelligent way.

And now is the time to start.

The true value of Industry 4.0 and the Connected Factory isn't derived from the sheer volume of connections; it comes from creating more meaningful connections...

- Mike Granby, "Elements of success: What the Connected Factory needs to flourish in 2014" 13 Jan 2014, *Embedded Computing Design*

20. Andy Chatha, "Planning for the Industrial Internet of Things," ARC Advisory Group, 30 Jan 2014. http://www.arcweb.com/strategy-reports/2014-01-30/planning-for-the-industrial-internet-of-things.aspx

About *groov*

Designed for industrial use by a company with 40 years experience in the field, *groov* offers a remarkably easy way to put system information into the hands of the people who need it.

Simple to build and simple to use, *groov* operator interfaces supplement your current HMI by providing key data to authorized engineers, technicians, and managers on off-the-shelf smartphones and tablets.

Because it is designed on open standards (OPC-UA, HTML5, CSS3, SVG), the *groov* interface you build works with a wide variety of control systems and runs on *any* device that can use a modern web browser: smartphones and tablets from any manufacturer, computers from any manufacturer, even large-screen TVs that are web-enabled.

For more information, visit *groov*.com or contact Opto 22 Pre-Sales Engineering:

Phone: 800-321-6786 or 951-695-3000
Email: systemseng@opto22.com.

About Opto 22

Opto 22 was started in 1974 by a co-inventor of the solid-state relay (SSR), who discovered a way to make SSRs more reliable.

Opto 22 has consistently built products on open standards rather than on proprietary technologies. The company developed the red-white-yellow-black color-coding system for input/output (I/O) modules and the open Optomux® protocol, and pioneered Ethernet-based I/O.

In addition to SSRs, Opto 22 is probably best known for its high-quality SNAP PAC programmable automation controllers and I/O, all of which are manufactured and supported in the U.S.A. Because the company builds and tests its own products, Opto 22 guarantees all solid-state SSRs and I/O modules for life.

The company is especially attractive for its continuing policy of providing free product support, free training, free documentation, and free pre-sales engineering assistance.

For more information, visit opto22.com.