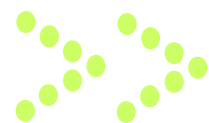


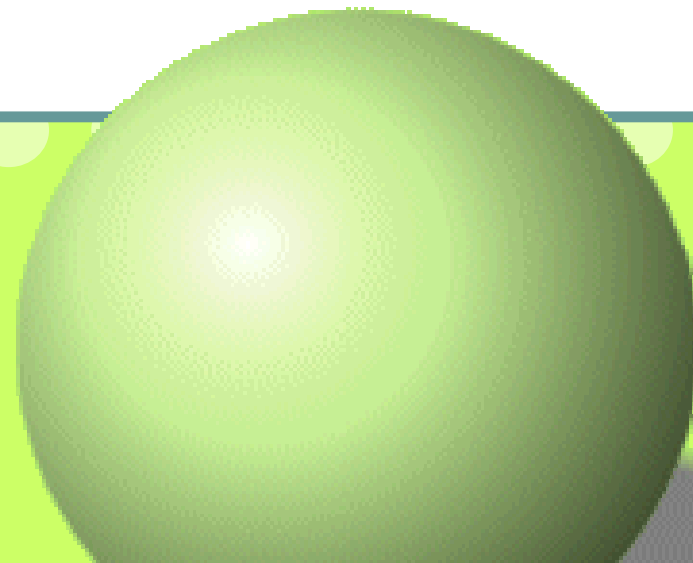
Cybersecurity in Control Systems (SCADA, DCS, and more) – Automobiles, Buildings and Power Grids



Matthew E. Luallen, President

m@sph3r3.com

Discover, realize,
maintain and protect
your cyber assets.

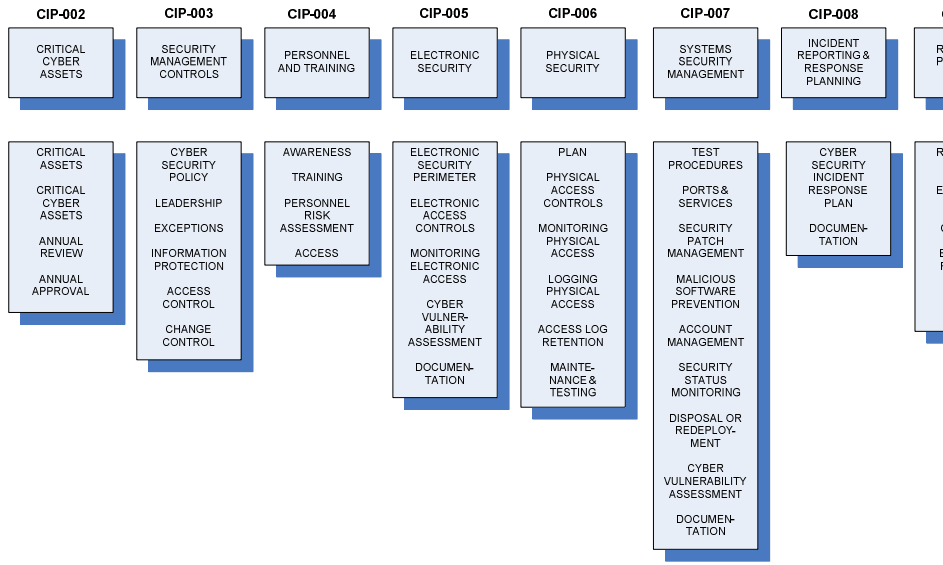


Where and what control systems are today

Automotive control systems research, history and why you should be concerned

Cyber in your data center's HVAC and the home application of smarter grid technology

Control centers, generation, transmission and distribution (Smart Grid) control systems concerns



NERC CIP discovery, architecture, and integration work for control systems within electric utilities

Further aided by years of experience performing Cyber Asset discovery at universities, government facilities, healthcare (a worthy set of adversaries)

GOAL: Seek help (research and integrators) for our expanding control system challenge.

Monitored by an iPhone ...

 **Auto**
BMW Develops IP-based Networking for Next Gen Vehicles
Brandon Hill (Blog) - December 3, 2007 4:51 PM

E-mail del.icio.us listen now 33 comment(s) - last by jconan.. on Jan 1 at 1:37 AM

Technology filters down to the automotive market

no stranger to high-tech in its vehicles. The German BMW owners around the introduction of the Windows driver information center in its iDrive, which has been popular with enthusiasts and auto journalists down to the 5-Series, 3-Series, 1-Series and X5.

The introduction of iDrive by many manufacturers have shown control schemes with a variety of control knobs and buttons and a variety of interior lighting -- more


looking to make another step in future automobiles with the vast array of networked features (etc.).

Nissan dials iPhone for car remote control

An iPhone application allows for remote monitoring of battery levels and control of air conditioning in electric cars

By [Martyn Williams](#), IDG News Service, 07/27/2009

 Share/Email  Tweet This  Comment  Print

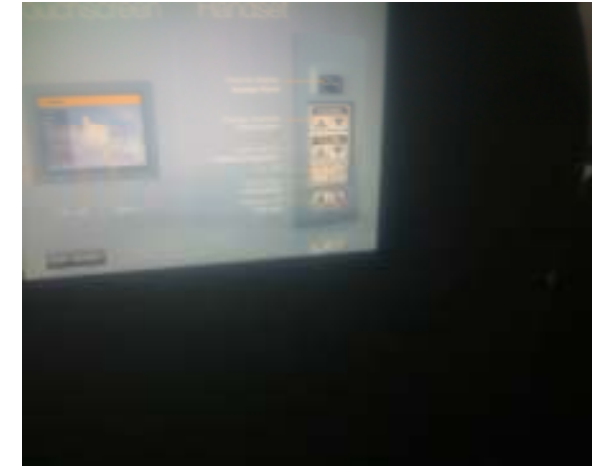
 Newsletter Sign-Up

Nissan has developed a prototype iPhone application that would allow electric car owners to dial into their vehicles and check battery levels.

The application, a working version of which was demonstrated by the company at its research facility in Yokosuka, Japan, links to the car's IT system to check the status of the Lithium Ion batteries that power the car.

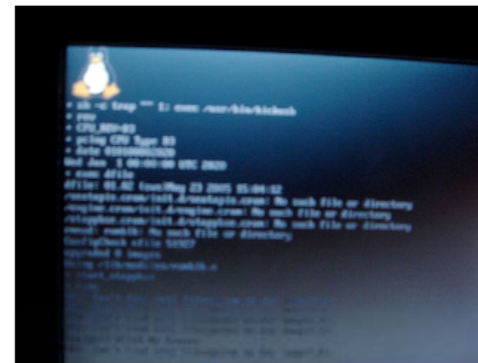
craft control systems ...

Special conditions are routinely developed and published in the normal certification program process whenever the FAA determines the current aviation regulations are inadequate to address a potential safety concern," he wrote, adding that, "the applicant is introducing new technology and proposing **more connectivity between passenger / cabin services and other airplane networks and systems** than on past airplane models in which aircraft networks and systems were more isolated (no or very limited connectivity between these networked systems). **The current regulations and guidance do not adequately address the security aspects of this additional connectivity."**



http://www.wired.com/politics/security/news/2008/01/dreamliner_security

<http://blog.wired.com/27bstroke6/2008/01/faa-responds-to.html>



- RTCA Home
- Annual RTCA
- RTCA Committees
- RTCA Governance
- Calendar of Events
- List of Available Documents
- RTCA Online Store

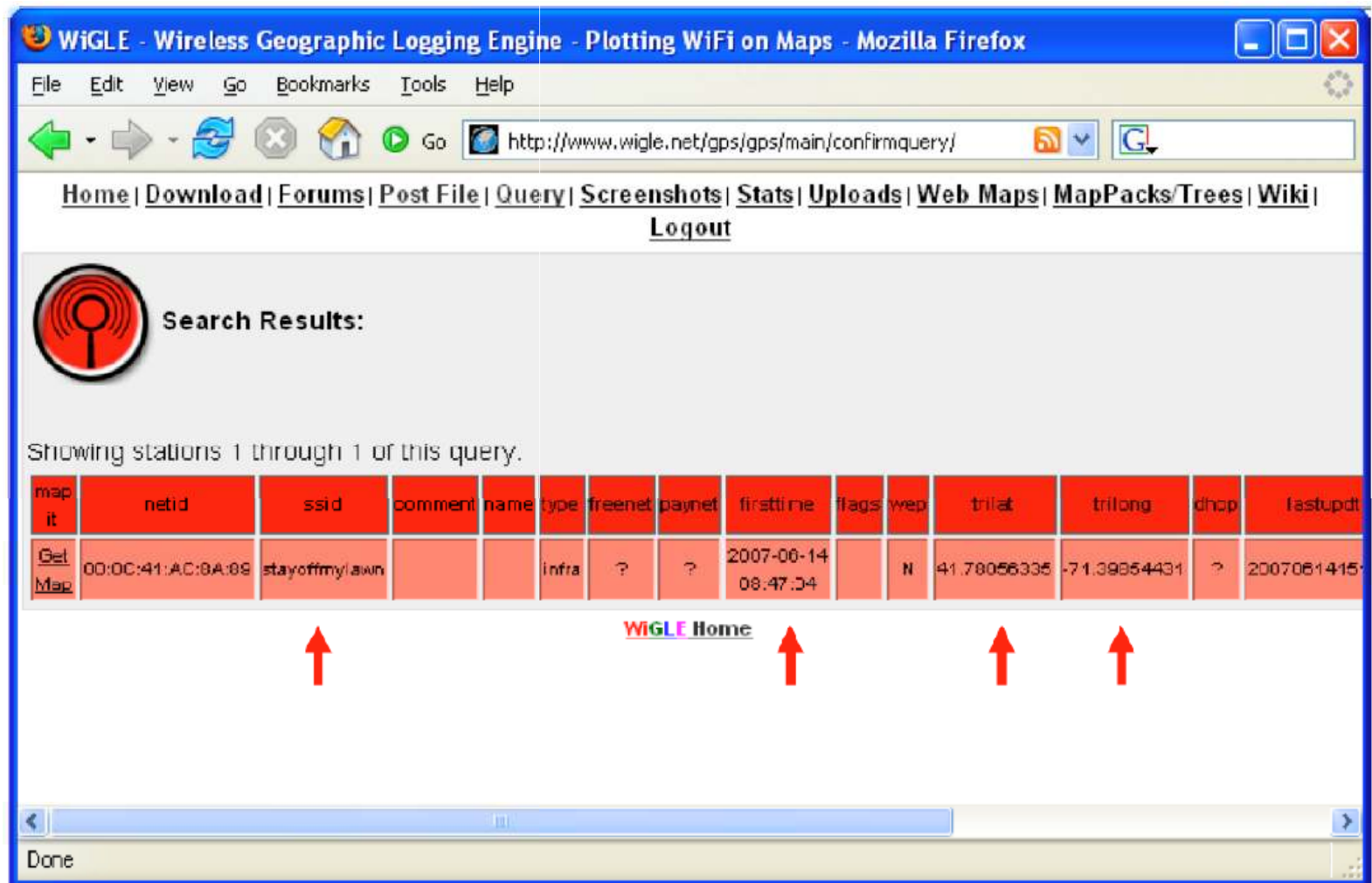
SC-214 (Joint with EUROCAE WG-78) Standards for Air Traffic Data Communication Services

SC-214 was established at the request of the Federal Aviation Administration to develop standards to define the safety, performance and interoperability requirements for Air Traffic Services (ATS) supported by data communications. Data Communications in support of the NextGen Air Transportation System and Single European Sky ATM Research (SESAR) Initiatives will introduce services that allow evolution from the current workload intensive, voice based air traffic control concepts, to collaborative, management by-exception operations. Advanced data links between ground and airborne systems are envisioned to increase sector-based traffic capacity allowing greater user access and more efficient flight routing.

Committee Info	Products/Remarks	Project Completion	Links
Established: March 22, 2007	<i>Safety and Performance Standard for Advanced ATS Data Communication</i>	December 2011	Last Meeting 3 - 7 May 2010

More than you think ...

How many RFIDs do you have?



The screenshot shows a Mozilla Firefox browser window displaying the WiGLE website. The page title is "WiGLE - Wireless Geographic Logging Engine - Plotting WiFi on Maps". The address bar shows the URL "http://www.wigle.net/gps/gps/main/confirmquery/". The page content includes a navigation menu with links like Home, Download, Forums, Post File, Query, Screenshots, Stats, Uploads, Web Maps, MapPacks/Trees, Wiki, and Logout. Below the navigation is a search results section with a red circular icon and the text "Search Results:". It states "Showing stations 1 through 1 of this query." and displays a table with the following data:

map it	netid	ssid	comment	name	type	freenet	paynet	firsttime	flags	wep	trilat	trilong	dhcp	lastupdt
Get Map	00:0C:41:AC:9A:09	stayoffmylawn			infra	?	?	2007-06-14 08:47:34		N	41.78056335	-71.39854431	?	2007061415

Below the table, there are four red arrows pointing upwards to the columns: "ssid", "firsttime", "trilat", and "trilong". The text "WiGLE Home" is visible below the table.

Everything without wires ...

SensiLink™ - Middleware to bridge Wireless Sensor Networks with SCADA systems, HMI, GIS, and Custom Applications

SensiLink™ Benefits:

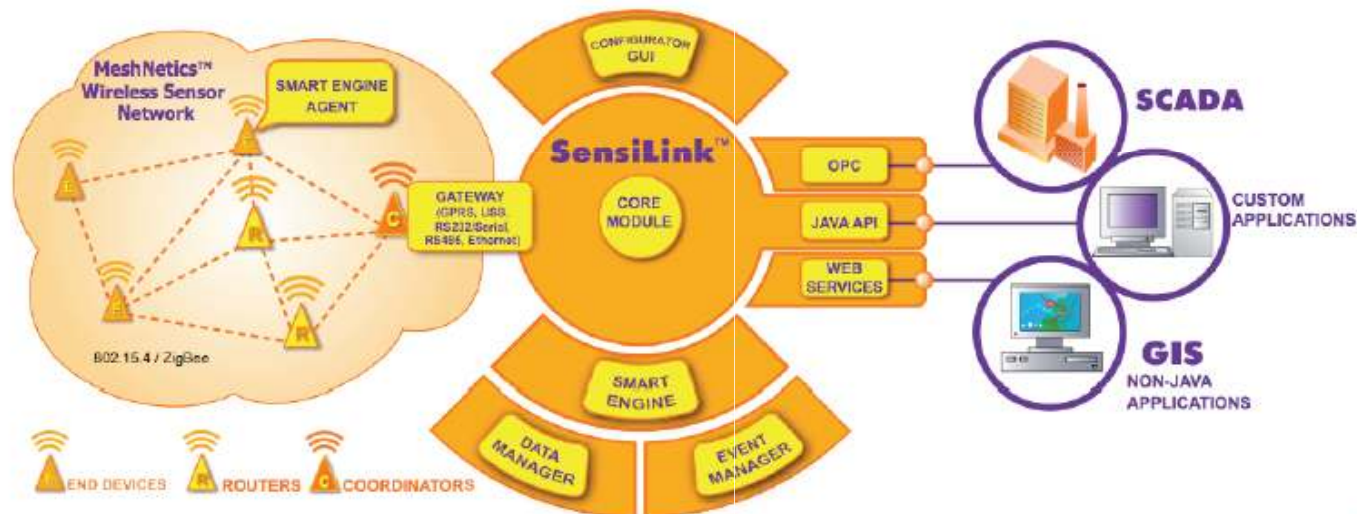
- Powerful external APIs
- Scalable Architecture
- Distributed Intelligence

SensiLink™ is a software suite that links wireless sensor networks with enterprise applications, such as SCADA (Supervisory Control and Data Acquisition) systems, HMI (Human Machine Interfaces), GIS (Geographic Information Systems), IP-based and custom applications. Thanks to OPC, Web Services and Java APIs, SensiLink™ serves as a powerful gateway between wireless sensor networks and these applications.

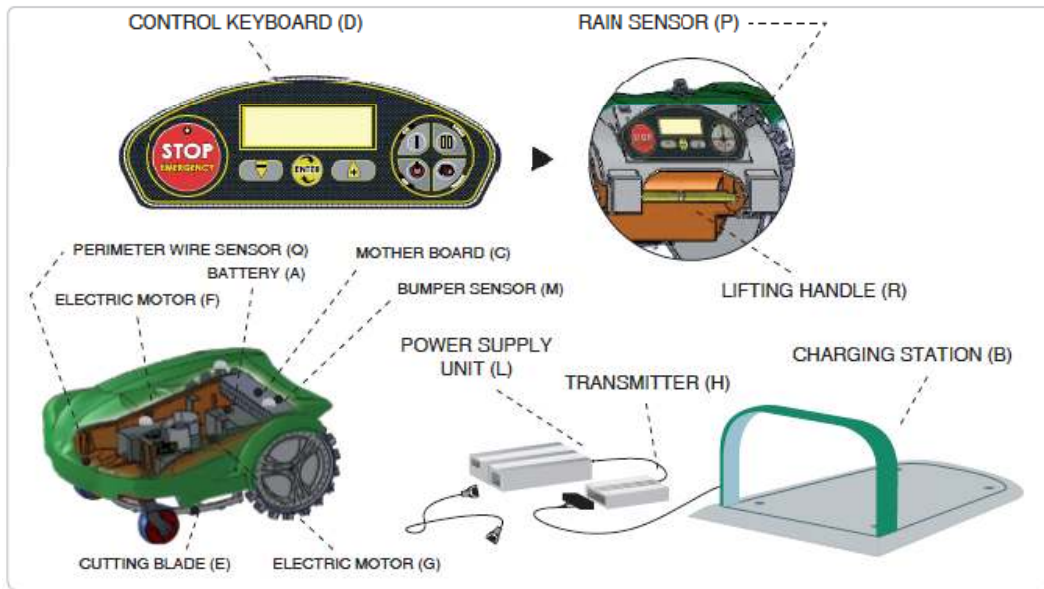
Target Applications:

- Industrial automation
- Asset monitoring
- Building automation
- Telemetry
- Security systems
- HVAC control
- Oil & gas industry

Wireless sensor network features eZeeNet stack embedded software, deployed on the nodes. Based on TinyOS open-source operating system, eZeeNet stack ensures wireless connectivity and forms self-organizing, self-healing star, cluster tree or mesh networks. The network layer of eZeeNet stack fully supports ZigBee specifications. Distributed intelligence is introduced in the network. Installed on the sensor nodes, Smart Engine software performs preliminary computations, which reduces unnecessary data traffic within the network and increases battery life. Sensor data collected from the nodes is channeled through RS232, RS485, USB, Ethernet or GPRS gateway to the server, running SensiLink™ software. Additionally SensiLink™ offers user-friendly graphic interface to facilitate easy network management. Data and event management modules are also available.



Equipped home lawnmowers ...



Settings		
Alarm	Enables or disables the acoustic alarm	<input type="checkbox"/> Enable <input type="checkbox"/> Disable
Rain sensor	Determines the behaviour in case of rain	<input type="checkbox"/> Restart <input type="checkbox"/> Pause <input type="checkbox"/> Disable
Auto setup	Enables or disables the "lawn mowed" recognition	<input type="checkbox"/> Enable <input type="checkbox"/> Disable
Remote control	Sets the Remote Control to drive the robot	<input type="checkbox"/> None <input type="checkbox"/> Pair bluetooth <input type="checkbox"/> Pair radio
Sound	Allows turning off the acoustic sound when the robot is in the charging station	<input type="checkbox"/> Enable <input type="checkbox"/> Disable
Date	Sets the date	
Time	Sets the time	

[home](#) [products](#) [accessories](#) [review](#) [manual](#) [faq](#) [gallery](#) [news](#) [testimonials](#) [forum](#) [order](#) [contact](#)

Toll-Free 7 Days a Week
(888) 483 0063

[LawnBott Models](#) [Why purchase a LawnBott](#) [Why choose LawnBotts.com](#)

FREE Shipping
30% OFF
LOWEST PRICES Guaranteed

Compare LawnBott Lawn Mowers
Robotic Lawn Mower Features

- Quiet, automatic mowing and self-charging
- Go green - no gas, no oil, no pollen
- Obstacle detection for trees and objects
- Automatic rain / sprinkler response system
- Safe robotic lawn mowers - CPSC accepted
- 30 degree hills are no problem
- Save time and money

[More >](#)

LawnBotts.com
 Award Winning Dealer - Sales and Service 2008
 Consumer Search Recommended Dealer

consumersearch
 LawnBottReview.com
 Expert Reviewer

[LawnBott LB3010](#) [LawnBott LB3210 / Evolution](#) [LawnBott LB2110 / Professional](#) [LawnBott LB1200](#)

LawnBotts.com - Authorized LawnBott Dealer of North America

h "GoToMyHMI.com" ...



GoToMyHMI

Your HMI-Gateway™ in the Cloud

Secure, Easy & Fast
Login to access your HMI

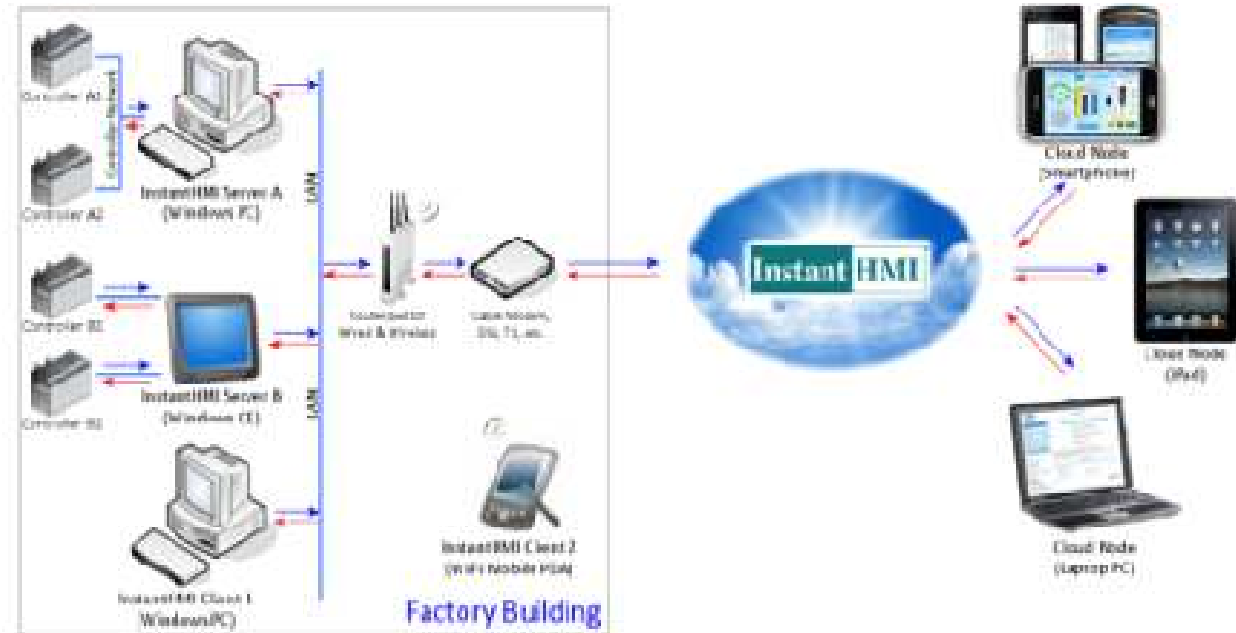
Customer ID:

User Name:

Password:

Session Duration:

[Help](#) | [Forgot Password?](#) | [Live Demo](#)



Standards and regulations ...

NERC CIP v1, v2, v3,
v4, ...

ISA S99

ISO 27001

NIST SP 800-53 r3,
800-82

NRC

IEC 62351

- NNSA
- DoD 8500.1
- IEEE P1686
- IEEE P1711
- IEC 61850 (Cigre B5.38)

- http://www.us-cert.gov/control_systems/csstandards.html

Information Reliability Standards

CIP-002

CRITICAL
CYBER
ASSETS

CRITICAL
ASSETS
CRITICAL
CYBER
ASSETS
ANNUAL
REVIEW
ANNUAL
APPROVAL

CIP-003

SECURITY
MANAGEMENT
CONTROLS

CYBER
SECURITY
POLICY
LEADERSHIP
EXCEPTIONS
INFORMATION
PROTECTION
ACCESS
CONTROL
CHANGE
CONTROL

CIP-004

PERSONNEL
AND TRAINING

AWARENESS
TRAINING
PERSONNEL
RISK
ASSESSMENT
ACCESS

CIP-005

ELECTRONIC
SECURITY

ELECTRONIC
SECURITY
PERIMETER
ELECTRONIC
ACCESS
CONTROLS
MONITORING
ELECTRONIC
ACCESS
CYBER
VULNER-
ABILITY
ASSESSMENT
DOCUMENT-
TATION

CIP-006

PHYSICAL
SECURITY

PLAN
PHYSICAL
ACCESS
CONTROLS
MONITORING
PHYSICAL
ACCESS
LOGGING
PHYSICAL
ACCESS
ACCESS LOG
RETENTION
MAINTEN-
ANCE &
TESTING

CIP-007

SYSTEMS
SECURITY
MANAGEMENT

TEST
PROCEDURES
PORTS &
SERVICES
SECURITY
PATCH
MANAGEMENT
MALICIOUS
SOFTWARE
PREVENTION
ACCOUNT
MANAGEMENT
SECURITY
STATUS
MONITORING
DISPOSAL OR
REDEPLOY-
MENT
CYBER
VULNERABILITY
ASSESSMENT
DOCUMENT-
TATION

CIP-008

INCIDENT
REPORTING &
RESPONSE
PLANNING

CYBER
SECURITY
INCIDENT
RESPONSE
PLAN
DOCUMENT-
TATION

CIP-009

RECOVERY
PLANS FOR
CCA

RECOVERY
PLANS
EXERCISES
CHANGE
CONTROL
BACKUP &
RESTORE
TESTING
BACKUP
MEDIA

defined by Princeton ...

The screenshot shows a Windows Internet Explorer browser window with the title "define:virtual - Google Search - Windows Internet Explorer". The address bar contains the URL "http://www.google.com/search?hl=en&defl=en&q=define:virtual&sa=X&oi=...". The search bar contains the text "define:virtual" and a "Search" button. Below the search bar, the "Web" tab is selected, and the search results are displayed. The first result is a definition of "virtual(a)" from WordNet at Princeton University. The definition is highlighted with a black box.

Web Images Products News Maps Gmail more Sign in

Google define:virtual Search Advanced Search Preferences

Web

Related phrases: [virtual reality](#) [virtual memory](#) [virtual private network](#) [virtual machine](#) [virtual server](#) [virtual image](#) [virtual circuit](#) [java virtual machine](#) [virtual community](#) [virtual terminal](#)

Definition

- **virtual(a):** being actually such in almost every respect; "a practical failure"; "the once elegant temple lay in virtual ruin"
- virtual(a): existing in essence or effect though not in actual fact; "a virtual dependence on charity"; "a virtual revolution"; "virtual reality"
wordnet.princeton.edu/perl/webwn
- Something which is a representation rather than the real thing. In advertising, the word "virtually" means "almost."
www.medialit.org/reading_room/article565.html
- Existing only in software.
www.tagnet.org/digitalhymnal/en/glossary_m-z.html

Internet 100%

Security (1 of 2)



security

Search

[Advanced Search](#)
[Preferences](#)

Web Books Groups News Personalized Results 1 - 10 of about 839,000,000 for security [definition]. (0.25 seconds)

What does **security** mean for process control, DCS, SCADA and specifically the Bulk Power control systems?

Protection of authentic and accountable control

Assurance of information integrity

Timeliness of transmission and receipt of data

Confidentiality and classification of information

Security (2 of 2)

Google

security

Search

[Advanced Search](#)
[Preferences](#)

Books Groups News Personalized Results 1 - 10 of about 839,000,000 for security [definition]. (0.25 seconds)

24X7

What does security mean for process control, DCS, SCADA and specifically the Bulk Power control systems?

Protection of authenticity and accountability control

Assurance of information integrity

Timeliness of transmission and receipt of data

Confidentiality and classification of information

Automation is everywhere, centralized control of local or remote field devices provides the “controlled” system of disparate cyber assets

- Transportation (Automobile, Trains, Aircraft, Construction, Farm Equipment, Pipelines, Boats)
- Fresh Water / Waste Water
- Electric Generation, Transmission and Distribution
- Oil Wells and Refineries
- Home and Building Automation (HVAC, Security, Location Awareness)
- Manufacturing Facilities
- Amusement Parks

Essentially where the **cyber and physical world meet.**

Experimental Security Analysis of a Modern Automobile

www.autosec.org

– Car Shark

Table III. Engine Control Module (ECM) DeviceControl Packet Analysis. This table is similar to Table II.

Packet	Result	Manual Override	At Speed	Need to Unlock [†]	Tested on Runway
07 AE ... 25 2B	Engages Front Left Brake	No	Yes	Yes	✓
07 AE ... 20 88	Engages Front Right Brake/Unlocks Front Left	No	Yes	Yes	✓
07 AE ... 86 07	Unevenly Engages Right Brakes	No	Yes	Yes	✓
07 AE ... FF FF	Releases Brakes, Prevents Braking	No	Yes	Yes	✓

Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study

<http://ftp.cse.sc.edu/reports/drafts/>

“There have been millions of vehicles installed with TPMS over the past 15 years. TPMS is a legislated safety system required on 100% of U.S. vehicles beginning in 2008, and similar legislation is being developed in Europe and the Asia-Pacific countries ... So don't worry. Tire pressure monitoring systems are secure.”

– Sept. 2010 : Schrader Electronics Ltd.

Interference



OPERATING EXPERIENCE SUMMARY

Issue Number 2008-06; Article 2: Radio Frequency Interference Triggers Nuclear

Radio Frequency Interference Triggers Nuclear Plant Shutdown

2

The increasing use of advanced analog- and microprocessor-based instrument and control systems in reactor protection and other safety-related systems has introduced concerns about creating additional noise sources. Equipment in such systems is very susceptible to both electrical noise and Radio Frequency Interference (RFI). The most recent example of RFI-related issues is the March 23, 2008, event in which a digital camera triggered a shutdown at Indian Point Nuclear Power Plant in Buchanan, New York (Figure 2-1).

On March 23, 2008, signals from a worker's digital camera caused an emergency shutdown of the reactor at the Indian Point Power Plant just 2 days before a scheduled refueling shutdown. When the camera was turned on too close to a control panel, RFI interfered with a boiler pump that provided water to four steam generators, causing the water levels to drop, thus resulting in an emergency shutdown. No radiation was released, but the 2-day work stoppage cost Entergy Nuclear (Entergy), the licensee, approximately \$2 million. (www.wabc.com, June 25, 2008)

Hacker Disables More Than 100 Cars Remotely

Kevin Poulsen March 17, 2010 | 1:52 pm | Categories: Breaches, Crime, Cybersecurity, Hacks and Cracks

More than 100 drivers in Austin, Texas found their cars disabled or the horns honking out of control, after an intruder ran amok in a web-based vehicle-immobilization system normally used to get the attention of consumers frequent in their auto payments.

Police with Austin's High Tech Crime Unit on Wednesday arrested 20-year-old Omar Ramos-Lopez, a former Texas A&M Center employee who was laid off last month, and reportedly sought revenge by bricking the cars sold from the dealership's four Austin-area lots.



SNAP ON SOLUS SCANNER DOMESTIC & ASIAN 10.2 SOFTWARE



Item condition: --
Time left: **4d 09h** (Oct 17, 2010 15:29:45 PDT)
Bid history: 20 bids

Current bid: **US \$1,075.00**
Reserve not met

Your maximum bid: US \$ **Place bid**
(Enter US \$1,100.00 or more)

Price: **US \$1,999.00** **Buy It Now**

[Add to Watch list](#)

PLX Kiwi Wifi OBD2 Automotive Diagnostic for iPhone

KL01
Wifi



Item condition: New
Quantity: 1 More than 10 available
Price: **US \$148.79** **Buy It Now**
[Add to Watch list](#)

Returns: 30 day money back | [Read details](#)
Shipping: [Read item description or contact seller for details.](#) [See more services](#)
See all details
Estimated delivery time varies. Seller ships within 1 day.

eBay Buyer Protection
eBay will cover your purchase price plus original shipping.
[Learn more](#)

Control Systems

Farm / Construction Equipment

- John Deere's JDLink
- AGCO's AgCommand
- Raven's Slingshot
- Trimble's Connected Farm



Research

- None known at this time.

IEEE 802.15.4

Initially released in 2004

- ZigBee-2006, encryption, MIC support
- ZigBee-2007, new home and business automation
- ZigBee-PRO, security model with "trust center"

Operates in the 2.4 GHz band (common)

- Also at 900 MHz (N. America), 850 MHz (Europe)

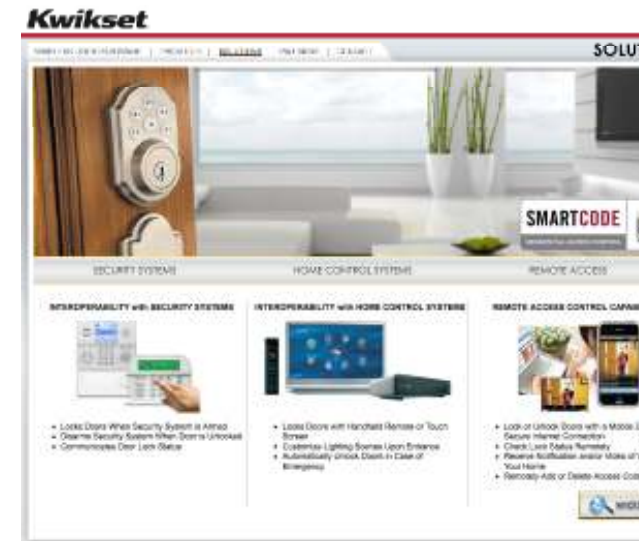
Modulation is DSSS – similar to 802.11b

- Sixteen 5 MHz channels, 11=2.405 GHz,
26=2.480 GHz

Hotel Online
News for the Hospitality Executive

Next-Generation RFID Lock System Implemented in 5,900 Rooms
at CityCenter in Las Vegas

KABA RFID Installation Delivers Future-Focused Guest Service Benefits for Luxury Resort



killerbee

Framework and tools for exploiting ZigBee and IEEE 802.15.4 networks

[Project Home](#) [Downloads](#) [Wiki](#) [Issues](#) [Source](#)
[Summary](#) | [Updates](#) | [People](#)

KillerBee is a Python based framework and tool set for exploring and exploiting security of ZigBee and IEEE 802.15.4 networks. Using KillerBee tools and a compatible IEEE 802.15.4 radio interface, you can eavesdrop on ZigBee network replay traffic, attack cryptosystems and much more. Using the KillerBee framework you can build your own tools, implement ZigBee fuzzing, emulate and attack end-devices, routers and coordinators and much more.

Honeywell, Siemens Apogee, Kwikset Smartcode, ...

Shared Infrastructure (Municipality, et. al.)

Default Settings

Distribution Automation / Smart Grid / Expanding Edge Automation

Communication Backchannels (Virtualization, Administration, and Wireless)

Break Fix Scenarios with Bolt-on Technologies

Municipality control networks may go well beyond expectations (fresh water, waste water, transmission, generation, ...)

Multi-owner facilities (substations, split location hydro generation)

Physical site usage (cellular antennas, office building, bathrooms, static keys)

Point: **Expansive operational boundaries**

Many systems have enabled additional services that are not necessary for “emergency” or “normal” operations

Traditional ICS IEDs do not generate security event logs and do not allow disabling unnecessary services

Vendors will reset systems to factory defaults while troubleshooting

Point: Vendors must provide flexibility in limiting unnecessary services and modifying default configurations.

Bandwidth Edge Automation

Not directly under the BES / NERC CIP regulations

Smarter Grid touchpoints are well beyond just electric utility boundaries

Examples

- MGM City Center 22k Zigbee devices
- Home automation (Insteon, X10, ...)

Point: **The edge will be automated by electric utilities, businesses and residential.**

Wide area connectivity (generation, substations, control centers, ISOs, business network, remote support)

- NAT / Split Tunnel Concern
- Expansive trust network

Unknown communication channels between hosts

Virtualization

- Host VM may not be considered Critical Cyber Asset while guest VMs are considered CCAs
- Shared SAN across trust zones (see first point)
- Use P2V tools to make an operational control system on a USB stick

System Administration (RS232, Infrared, Ethernet with lower security context)

KVM, UPS, Vendor Remote Access

Ethernet over Category 3

Wireless is everywhere : 802.11; 900 Mhz; Cellular GSM A5/1 Cipher

Wireless (USRP2 SDR opened door)

Bolt-on solutions are integrated throughout system lifecycle

- Break / Fix Scenarios
- New Features

Additional PLCs and communication gateways added

- Opto22 Snap-PAC
- Communication Bridges
 - 900 Mhz (only need same hardware to decode/inject)
 - 802.11 / Zigbee (review KillerBee)
 - Modbus to Ethernet/TCP

Point: **Contain control networks**

Build with a moat (control)

- Separate trust levels / Security Enclaves
- Understand how the moat (control) works
- Define trusted methods to cross the moat
- Strongly authenticate any attempted moat crossing
- Isolationism provides protection



* Nijo Castle
Kyoto, Japan

- “Computer Virus Strikes Space Station”
- August 27, 2008: Tariq Malik [space.com](#)
- A virus designed to swipe passwords from online gamers has inexplicably popped up in some laptop computers aboard the international space station.
- The low-risk virus was detected on July 25, but did not infect the space station's [command and control computers](#) and poses no threat to the orbiting laboratory, NASA officials said.

We need a mechanism to define varied operational states of a facility and an operational / cyber architecture to support it

- Cyber capability X is unavailable now invoke manual operation X
- As rings of the moat are directly hit, manually operations increase until such time the system is back to fully functional

No wireless communications (possibly even removing microwave / cellular for specific situations), No permanent OSI layer 1 inbound from untrusted sources

Profile control loop traffic immediately, Review ladder / automation logic

Monitor control system work in other verticals (eg. Automobile CAN Communications – or any other “easy” reference source)

Review ability to utilize data historians for cross correlated cyber / physical activity

**YOU MUST IMPLEMENT STRICT CHANGE MANAGEMENT CONTROLS
CONCLUSIVE OF ENSURING CYBER SECURITY REVIEW IN THE PROCUREMENT
PROCESS AND ALL SYSTEM CHANGES**

ur help?

Communications Protocols Assessments

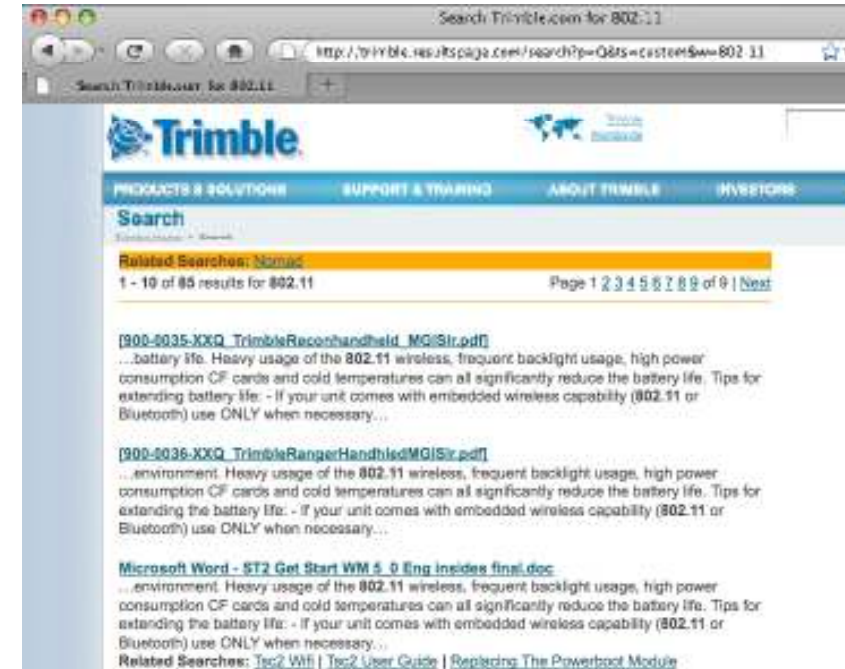
Control System Individual Device and As Built Assessments

... Many more.

Assessment Methodology

Documentation

- Vendor
- FCC ID or similar international registration



Reference Source

- Difficulty depends on accessibility of control system deployments

Monitoring and analysis tools

- Hobbylab USB Oscilloscope and Logic Analyzer
- USRP2 Software Defined Radio with appropriate daughter boards



PC USB Oscilloscope is a great tool for your microcontroller projects. Simply connect the device to the computer USB port, run the Win application and you can analyze the UART, SPI, I2C and I-Wire signals. In the same box you get Oscilloscope, Logic analyzer, Spectrum Recorder and Logic generator with a lot of functionalities for the price!



Built Assessments

Vendor, Integrator and Asset Owner Education

Local protective controls

Default settings

Administrative Modes

Firmware / Software Updates

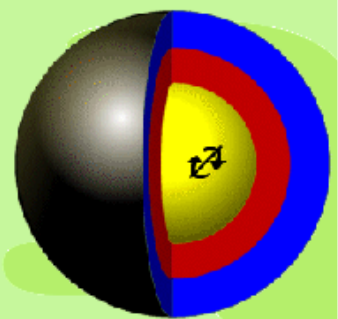
Software vulnerabilities

Forensics

Open Discussion

011011110111001001111001011010000111100001101101011011000110111101101111

sph3r3, LLC.



Evolving Strategy

“... delivering the information solutions required by the digital enterprise.”

Matthew E. Luallen
President and Principal Consultant

P: 312.375.4715
E: m@sph3r3.com

CISSP, CCIE, GSEC
MCSE, MS_CS

sph3r3.com/m.html