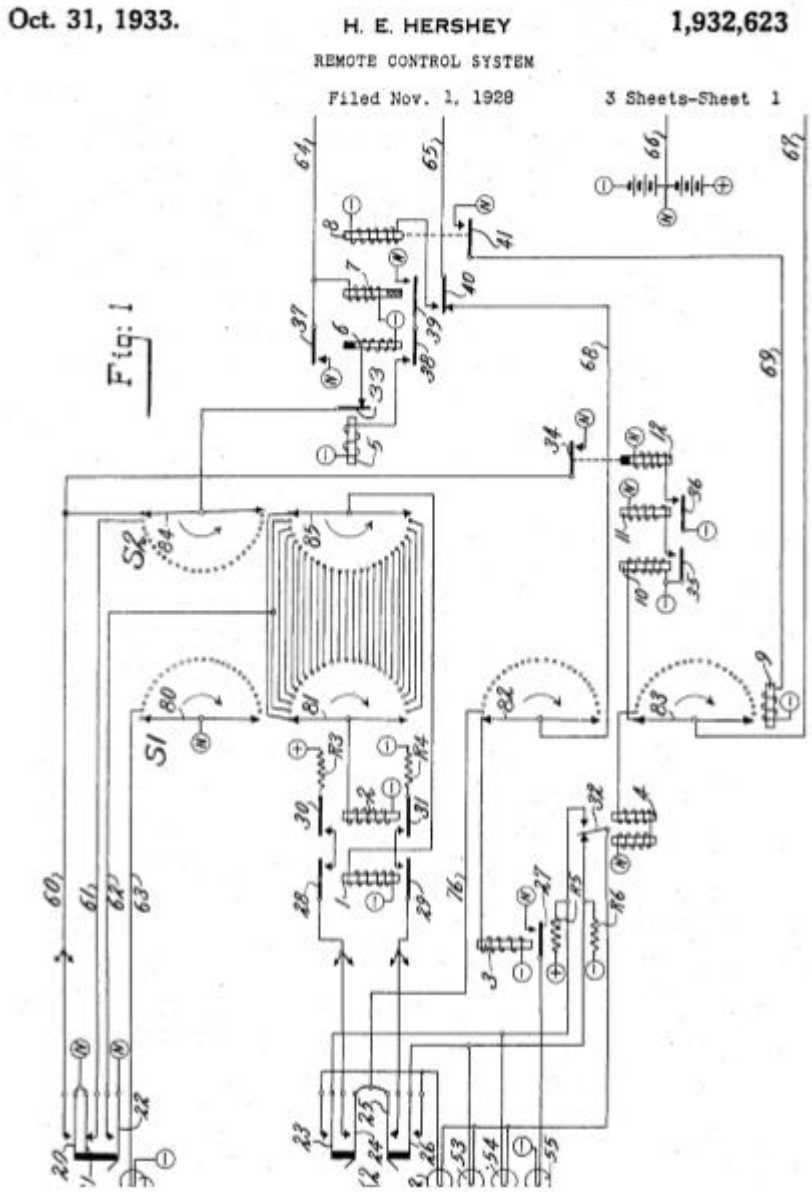
Strengthening SCADA Security

Information Security Inc. (ISI)
Noel Matchett
John Hershey

Remote process control has roots in the telephone industry

•"Early SCADA systems provided remote indication and control of substation parameters using technology borrowed from automatic telephone switching systems. As early as 1932, Automatic Electric was advertising "remote-control" products based on its successful line of "Strowger" telephone switching apparatus." from http://www.transmission-line.net/2011/05/history-of-scada-supervisory-control.html

•Opposite is a drawing from US Patent 1,932,623 "Remote Control System" held by Strowger Automatic. The inventor was Harry E. Hershey (John Hershey's uncle) who was a prodigious inventor for Automatic Electric.

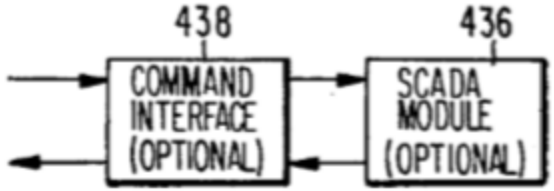


SCADA - the emergence of the term

Supervisory Control and Data Acquisition (SCADA) became an established data tool in the early 1960's. Remote sensing was made possible and desirable due to sensors, microprocessors, and communications. The emergence of SCADA techniques promised awareness and efficiency of remote processes through distant monitoring and adjustment.

- One of the earliest mentions of the term "SCADA" was in US Patent 4,264,960 "System for controlling power distribution to customer loads" issued to Sangamo Weston, Inc.
- In their patent we find

  "The *SCADA* module 436 is also optional and comprises a supervisory control and data acquisition system, which is a higher level computer that can control the MCS [Master Control Station]. A command interface 438 may be required for *SCADA* module 436."



But can we trust in SCADA?

•As SCADA networks grew, there also grew a realization that the SCADA system itself might come under attack. The field had become wide open with hundreds of protocols, many of which were kept under wraps and not extensively evaluated.

•Sandia produced a Laboratory Directed Research and Development report, SAND2002-0729, Printed April 2002. Some of its observations are cited in the right-hand block.

- The control systems [SCADA] that manage the Critical Infrastructures (CI) are vulnerable to physical and cyber damage.
- One of the more important problems in SCADA security is the relationship between the cyber and physical vulnerabilities. Cyber security and physical security continue to be treated as separate issues rather than as a part of a larger complex. Cyber intrusion increases physical vulnerabilities, while, in the dual problem, physical tampering increases cyber vulnerabilities.
- Many of the recent changes to SCADA systems have come from advances in the computing and telecommunications industries. The evolving SCADA systems are becoming more efficient and cost effective, but arguably less secure.

Cyber Vulnerabilities are continually studied but what about Physical Attacks?

- While it is clear that there is ever increasing attention to software cybersecurity, it is less clear that there is a balanced approach to achieving overall cybersecurity which must include the physical equipment and its interface to the software and communications.
- In a Red Team Exercise, reported at SANS SCADA Summit in January 2008, on-site physical access was allowed. The conclusion, which was perhaps not overly surprising was that **"Physical Trumps Cyber Every Time."**

Physical attacks against SCADA systems can be mounted at many stages, for example:

- by providing malware hosting components to SCADA equipment manufacturers who would use them in building their product
- by an insider threat wherein hardware Trojan horses are inserted during SCADA equipment manufacture
- by an operative covertly penetrating operating SCADA equipment and replacing or modifying key protective measures

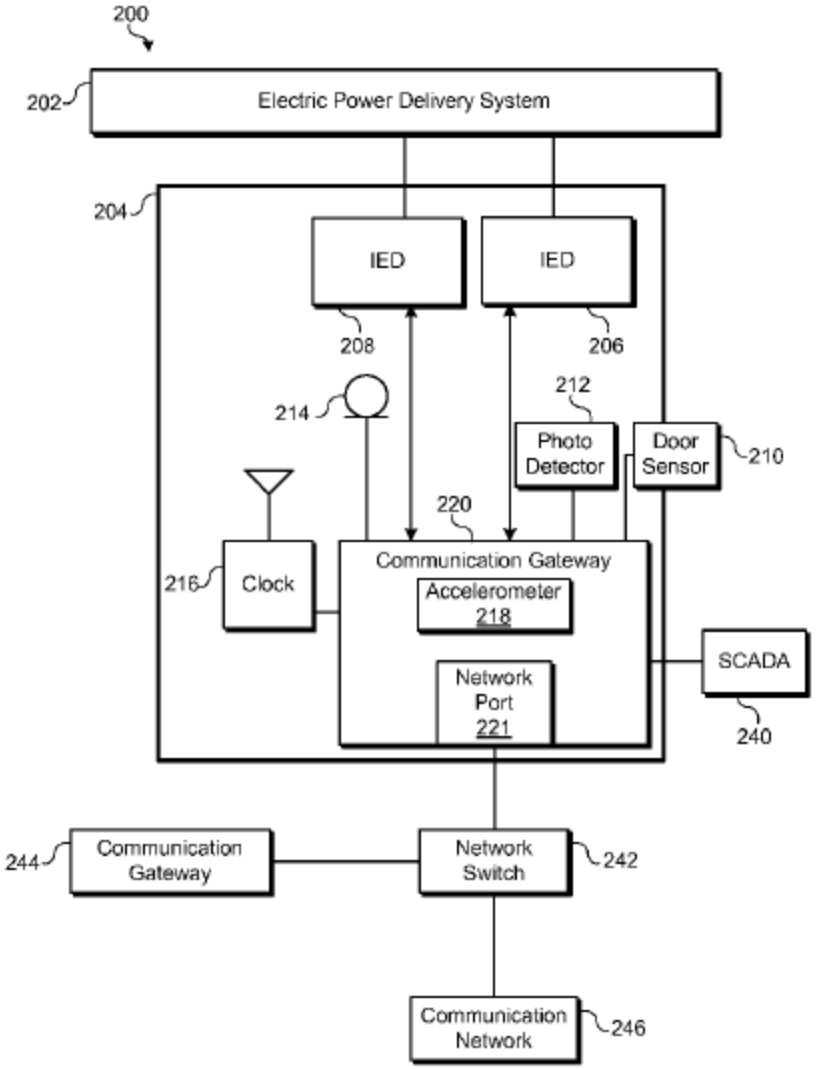
"*It is important to note that physical security and cybersecurity are intertwined and both are necessary to achieve overall security*." [1]

[1] Technology Assessment – Cybersecurity for Critical infrastructure Protection GAO-04-321 Page 3

"The vulnerability of field cabinets to physical tampering is a growing concern …" (senior product manager at Schweitzer Engineering Labs. in 2014)

•To detect unauthorized access to enclosure 204, communication gateway 220 may further be in communication with a door sensor 210 … [that] may be configured to signal communication gateway 220 if it detects opening of a door of the enclosure 204.

•… to detect unauthorized access to enclosure 204, communication gateway 220 may be in communication with a photo detector 212. The photo detector 212 may detect when the enclosure 204 is opened by a change in lighting within the enclosure 204 … The photo detector 212 may be configured to signal the communication gateway 220 when light is detected.



From Schweitzer's 2014/0109182 "Detection and Response to Unauthorized Access to a Communication Device."

ISI has a filing ready for a provisional patent , "Integrity Monitor,"

The application is for a system and method for monitoring the integrity of a remote site system or a portion thereof. The alarm conditions set for a sensor monitoring the integrity of the housing of the system is set on installation. The alarm conditions set for a sensor monitoring the remote site system or portion thereof may be set on installation or may be assumed following a learning period. An instance of an alarm is diarized with data comprising an encrypted record of the sensor's identification and its output.

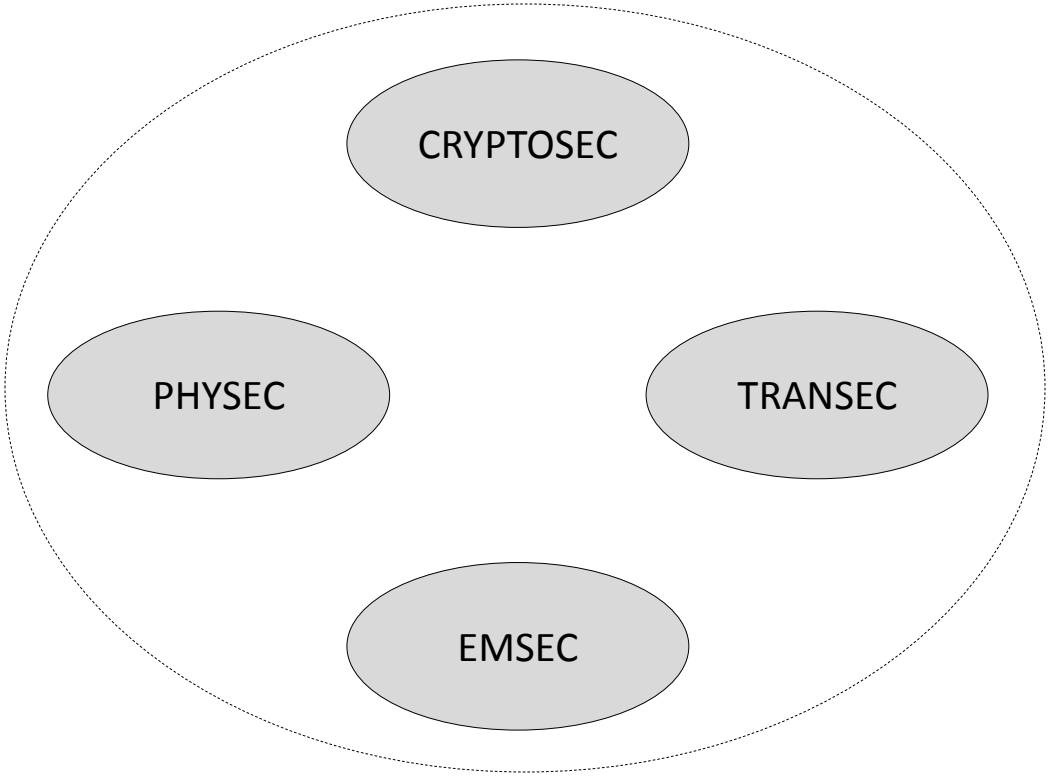
- ISI's Integrity Monitor is not meant to be a replacement to extant SCADA. Rather, it is intended to teach techniques that can be used to strengthen very critical Reporting & Control (R&C) functions. Its principles may do this by providing tamper detection and an interrogation protocol that does not reveal an alarm condition.
- The Integrity Monitor principles are organized about a balanced application of four fundamental pillars of R&C security.

Security is a conditions arising from a balanced application of essential elements

Elements essential to a critical Reporting & Control (R&C) System are:

- Cryptographic Security – the proper use of a sufficiently strong cryptoalgorithm
- Physical Security – the instantiation of sufficient tamper resistance/tamper detection materials and techniques
- Transmission Security – the denial of useful intelligence to an interloper from the study of enciphered traffic patterns from the R&C System
- Emanation Security – the denial of exploitable intelligence bearing incidental emanations from the R&C System

A balanced application incorporates and joins the four security arts:



Embodiments of ISI's Integrity Monitor incorporate all four of the R&C principles

- CRYPTOSEC
- PHYSEC
- TRANSEC
- EMSEC

A simple hardware example

- ISI believes a simple example of an embodiment of the Integrity Monitor and its interrogation protocol could be produced within a very short time
- A suitable simple example might be a door monitor that detects if a door to a secure area has been opened and if the Integrity Monitor has not been penetrated.