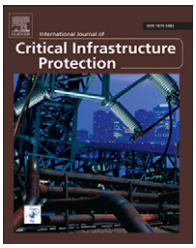
Available online at www.sciencedirect.com
SciVerse ScienceDirect
www.elsevier.com/locate/ijcip



Analysis and mitigation of vulnerabilities in short-range wireless communications for industrial control systems

Bradley Reaves[a], *Thomas Morris*[b,*]

[a]*Georgia Institute of Technology, School of Computer Science, 266 Ferst Drive Georgia 30332, United States*
[b]*Mississippi State University, Critical Infrastructure Protection Center, Electrical and Computer Engineering, 216 Simrall Engineering Building, Box 9571, Mississippi 39762, United States*

ARTICLE INFO

Article history:
Received 12 April 2011
Received in revised form
1 October 2012
Accepted 3 October 2012
Available online 11 October 2012

Keywords:
Industrial control systems
Wireless communications
Vulnerabilities
Mitigation

ABSTRACT

Industrial radios deployed in critical infrastructure provide a potential vector for attackers to penetrate control systems used in the food and agriculture, chemical, critical manufacturing, dams, energy, defense industrial base, government facilities, nuclear reactors, materials and waste, transportation and water sectors. Industrial radios offer convenience and flexibility in deployment while presenting cyber security challenges that wired communications do not. This paper presents a survey of literature related to wireless communications cyber security. The paper focuses on vulnerabilities and mitigations related to multiple industrial radio technologies deployed in control systems including IEEE 802.15.4, WirelessHART, ZigBee, Bluetooth, and IEEE 802.11. This paper also discusses how industrial radio vulnerabilities may be used as vectors for simple and complex attacks on control systems found in critical infrastructure. Finally, this paper provides a set of recommendations for securing wireless networks used in control systems.

1. Introduction

Modern society has become dependent on critical infrastructure including water treatment plants, nuclear power plants, electricity generation, distribution, and transmission, petroleum refining, gas pipelines, and chemical processing. Failure of these systems can lead to financial and property losses and physical harm to the citizenry. Many of these critical infrastructure use a common set of electronic control systems, collectively called industrial control systems (ICS), also known as supervisory control and data acquisition (SCADA) systems or process control systems (PCS), to manage complex and potentially dangerous processes. Industrial control systems are used internationally in the critical infrastructures of all countries to monitor sensors, to open and close valves, and to toggle switches remotely over a networked environment. Industrial control system networks have been shown to be vulnerable to intrusion and represent a significant weakness in global critical infrastructure.

Wireless networks are increasingly pervasive in industrial control systems. In a recent survey of control system operators [1], 43% of respondents indicated wireless networks were currently deployed in the industrial control systems they are associated with. An additional 23% intended to install wireless networks in the next 1–3 years. Wireless networks are used to add wireless sensor networks to existing industrial control systems to provide increased visibility to process data. Wireless networks are also used to provide short

*Corresponding author. Tel.: +1 662 325 3199; fax: +1 662 325 2298.
E-mail address: morris@ece.msstate.edu (T. Morris).

1874-5482/$ - see front matter © 2012 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.ijcip.2012.10.001

distance and long distance interconnections where adding wired networks are technically or financially infeasible. The aforementioned survey also addressed the prevalence of various wireless protocols available for use in industrial control systems. Respondents reported using IEEE 802.11, proprietary, WirelessHART, Bluetooth, and ZigBee wireless systems, and the relative prevalence of each system is shown in Table 1. Survey respondents use more than one type of wireless system, so the reports do not sum to 100%. Wireless systems, by their broadcast nature, are inherently less secure and less reliable than wired installations. Insecure wireless connections provide attackers with means to eavesdrop on control system communications and with means to penetrate control systems to inject illegitimate commands and responses. This paper provides background on industrial control systems and industrial control system networks including discussion on the types of wireless networks found in industrial control systems, classes of industrial control system attacks, and implications of various wireless network topologies. Next, an exhaustive survey of known cyber security vulnerabilities and exploits against IEEE 802.11, proprietary systems, IEEE 802.15.4 (used by WirelessHART and ZigBee), WirelessHART, Bluetooth, and ZigBee protocols is provided. In total 34 vulnerabilities are discussed. These vulnerabilities permit network penetration, reconnaissance, packet injection, denial of service, and man-in-the-middle attacks. The paper includes discussion of the impact of these vulnerabilities when exploited against industrial control systems. Impacts are grouped by attack class and detailed examples are provided. A set of recommendations for securing vulnerable wireless systems is also provided. Recommendations are grouped by general recommendations for all wireless systems, and specific recommendations for each surveyed wireless protocol. Finally, a discussion of future directions and conclusions is offered.

Table 1 – Wireless system usage in industrial control systems [1].

Wireless system	ICS prevalence (%)
IEEE 802.11	51.5
Proprietary systems	34.0
WirelessHART	23.0
Bluetooth	18.2
ISA 100-11a	4.4
ZigBee	1.5

2. Background

Fig. 1 shows an example network diagram of an industrial control system with multiple outstations, a control center, and a network connection to an enterprise network. The outstations include remote terminal units connected to sensors and actuators which connect to physical processes. RTU store control parameters and execute algorithmic code (such as ladder logic or C programs) to directly control the physical process. RTU may be programmable logic controllers (PLC), programmable automation controllers (PAC), intelligent electronic devices (IED), industrial computers, relays, or other types of programmable devices.

The control center shown in Fig. 1 includes multiple master terminal units (MTUs), a human–machine interface (HMI), a gateway, and a historian. The HMI and MTU provide a supervisory control and data acquisition functions. The HMI allows human operators to monitor and control physical processes. The HMI connects to the MTU which forwards HMI queries to the RTU and forwards RTU responses to the HMI. The MTU may also include programmable logic to automate supervisory control or data acquisition functions. For instance, the MTU may periodically query the RTU to collect process measurements for storage in the historian. The MTU may also execute supervisory control actions that leverage the MTU's wide area visibility across a larger control system. The control center includes a gateway device that provides a secure connection to a corporate enterprise

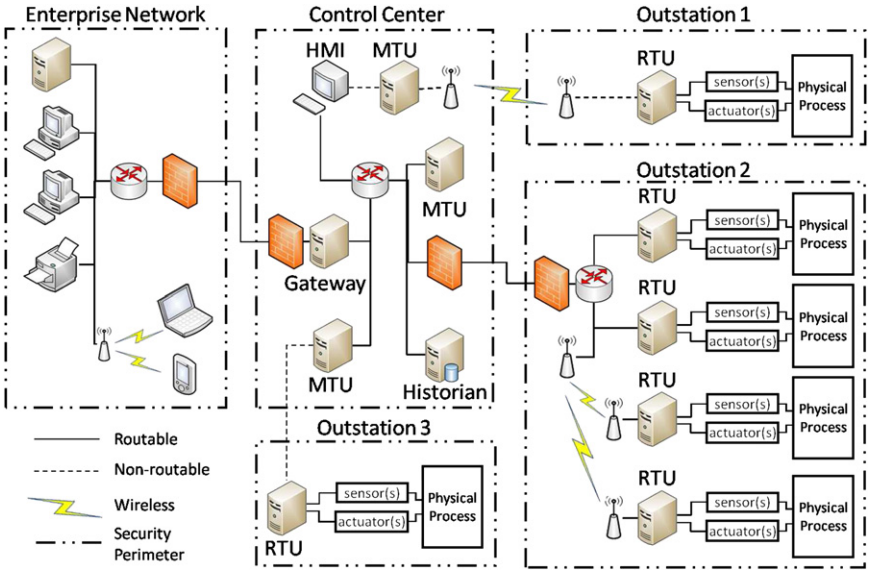


Fig. 1 – Example industrial control system network.