JPCERT/CC®

「制御系プロトコルに関する調査研究」
報告書＜目次＞

Control System Protocol Research Report

有限責任中間法人 JPCERT コーディネーションセンター

平成 20 年 6 月 24 日

DIGITAL BOND AND JPCERT/CC CONFIDENTIAL

Prepared by:

Charles Perine
Dale Peterson
Julian Rrushi

Digital Bond, Inc.
1580 Sawgrass Corporate Parkway, Suite 130
Sunrise, FL 33323

本調査報告書は、経済産業省の委託を受けたJPCERTコーディネーションセンターが、Digital Bond Inc.に依頼し調査・作成したものです。

本調査報告書の使用について、JPCERTコーディネーションセンターの事前の承諾を受けた場合を除いて、テキストやそれらに包含される内容(一部か全部を問わない)を複製・公開・送信・頒布・譲渡・貸与・使用許諾・転載・再利用できません。

JPCERT/CCロゴは、JPCERTコーディネーションセンターの登録商標です。その他各社の社名、製品名などは各社の登録商標または商標です。

Table of Contents

Executive Summary 5
Abbreviations 8
Protocol Use Scenarios 9
Attack and Threat Scenarios 12
  Why Focus on Ethernet, IP and TCP/UDP Protocols? 12
  Geography 15
  Complexity 15
  Vertical Markets 17
CC-Link IE 18
  History 18
  Typical Use 18
  Functions and Features 18
  Protocol Implementation 19
  Relation to Other Control System Protocols 19
  Published Vulnerabilities 20
DNP3 21
  History 21
  Typical Use 21
  Functions and Features 21
  Security Features 23
  Protocol Implementation 26
  Relation to Other Control System Protocols 27
  Published Vulnerabilities 27
EtherCAT 28
  Typical Use 28
  Functions and Features 28
  Protocol Implementation 29
  Relation to Other Control System Protocols 29
  Published Vulnerabilities 29
EtherNet/IP 30
  History 30
  Typical Use 31
  Functions and Features 31
  Security Features 32
  Protocol Implementation 33
  Relation to Other Control System Protocols 33
  Published Vulnerabilities 33
FL-net (OPCN-2) 34
  History 34
  Typical Use 34
  Functions and Features 34
  Protocol Implementation 35
  Relation to Other Control System Protocols 35
  Published Vulnerabilities 35
Foundation Fieldbus HSE 36
  History 36
  Typical Use 36

Copyright ©2008 Digital Bond,Inc. All rights reserved.

Functions and Features 36
Protocol Implementation..38
Relation to Other Control System Protocols...38
Published Vulnerabilities..38
IEC 61850 39
History...39
Typical Use 39
Function and Features 40
Security Features...44
Protocol Implementation...45
Relation to Other Control System Protocols...45
Published Vulnerabilities...46
Modbus TCP 47
History..47
Typical Use 47
Functions and Features 47
Security Features..49
Protocol Implementation..49
Relation to Other Control System Protocols..49
Published Vulnerabilities..50
OPC and OPC UA 51
Typical Use 51
Functions and Features 52
Protocol Implementation...53
Relation to Other Control System Protocols...53
Published Vulnerabilities...54
PROFINET 55
History..55
Typical Use 55
Functions and Features 55
Protocol Implementation..57
Relation to Other Control System Protocols..57
Published Vulnerabilities..57
Appendix A: Control System Published Vulnerabilities 58
GE Fanuc 58
Gesytec..61
ICONICS..62
LiveData...63
NETxAutomation...69
SISCO 70
Takebishi Electric 74
Wonderware...76
Appendix B: Control System Protocol List 78
Appendix C: References 85

Copyright ©2008 Digital Bond,Inc. All rights reserved.