

DeltaV™ Security Manual

Implementing Security on DeltaV Distributed Control Systems



To protect this information this public version only provides the manual's Table of Contents.

A full copy of this document is available in the Resources section of Emerson's Guardian Support Portal.

This manual is Emerson confidential and intended for use only by customers, employees, Impact Partners, and others who are responsible for providing security services to Emerson systems and products. This manual may be provided to potential customers as required to evaluate DeltaV security implementation. The distribution of this manual does not require a Non-Disclosure Agreement (NDA).

This manual must not be posted on public websites or redistributed, except as noted above, without permission from Emerson.



Table of Contents

1	Introduction	6
1.1	Purpose	6
1.2	Organization	7
1.3	Standards	7
1.3.1	Vendor compliance to the published security standards	7
1.4	Relevant documentation	8
1.4.1	Background reading.....	8
1.4.2	DeltaV documentation	9
1.4.3	Microsoft documentation.....	9
1.4.4	Third-party product documentation.....	9
1.5	Security and DeltaV system projects.....	10
1.6	Security Collaboration between IT and Operations Departments	11
1.7	Submitting Material for This Manual	13
1.8	Glossary.....	13
2	Security basics	15
2.1	Threats to control systems	15
2.2	Assets and compromises	15
2.3	Vulnerabilities	16
2.4	Control system architecture.....	16
2.5	Security policies and procedures.....	18
2.6	Defense-in-depth	19
2.7	Performing risk assessments	19
2.8	Security Hardening	20
3	DeltaV defense-in-depth strategy	21
3.1	Overview.....	21
3.2	Possible attack vectors.....	22
3.3	Deployment security environment expected for DeltaV systems	23
3.4	Physical security	25
3.5	Network topology	26
3.5.1	Network architecture.....	27
3.5.2	Access from the DMZ	28
3.5.3	DeltaV 2.5 Network.....	29
3.5.4	DeltaV Remote Network	30

3.5.5	DeltaV Inter-Zone Network	32
3.5.6	DeltaV Area Control Network (ACN)	33
3.5.6.1	Description	33
3.5.6.2	Connecting non-DeltaV computers to the ACN	35
3.5.6.3	Extending the ACN using wireless Ethernet bridges	35
3.5.7	DeltaV SIS Networks	36
3.5.7.1	DeltaV SIS with Smart Logic Solvers (SLS1508)	37
3.5.7.2	DeltaV SIS with Electronic Marshalling	38
3.5.8	DeltaV Virtualization Networks	39
3.5.8.1	Thin Client Network	41
3.5.8.2	Cluster Management Network	42
3.5.8.3	Storage Area Network	42
3.5.9	Active Directory Design for DeltaV	43
3.5.10	Printers.....	45
3.5.11	<i>WirelessHART</i> segments.....	46
3.6	Communications security	49
3.7	OPC UA (Unified Architecture).....	49
3.7.1.1	Security in DeltaV with OPC UA	50
3.7.1.2	Best Practices for Optimizing OPC UA Security in a DeltaV System	52
3.8	DeltaV Mobile	52
3.9	Secure First Mile.....	54
3.10	User account security	55
3.10.1	Account management.....	56
3.10.1.1	Centralized management of accounts	56
3.10.1.2	Account creation and maintenance	56
3.10.1.3	Operating system and account use	58
3.10.1.4	DeltaV account use.....	59
3.10.1.5	Account expiration	59
3.10.1.6	Removal of temporary accounts	60
3.10.1.7	Removal of unused accounts	60
3.10.2	Passwords	60
3.10.2.1	Complexity	60
3.10.2.2	Default passwords	61
3.10.2.3	Expiration period.....	63
3.10.2.4	Expiration prompt.....	63

3.10.2.5	Reuse.....	64
3.10.2.6	Password policy summary	64
3.10.3	Shared accounts.....	65
3.10.4	Installation-generated user accounts.....	65
3.10.5	Account activity logging	65
3.10.6	Logging into the DeltaV system.....	65
3.11	Device hardening	66
3.11.1	Digital Certificates.....	68
3.12	Security event handling.....	68
3.12.1	Event logging and reporting.....	68
3.12.1.1	General security event handling	68
3.12.1.2	User activities	69
3.12.1.3	Log of security events.....	69
3.12.1.4	Backup Activity Logging.....	69
3.12.2	System monitoring.....	70
4	DeltaV defense-in-depth components.....	71
4.1	External remote access applications	71
4.1.1	Overview.....	71
4.1.2	Security requirements specific to remote user access	72
4.1.3	Microsoft Remote Desktop	74
4.1.4	DeltaV remotely accessible applications	75
4.1.5	Emerson Smart Firewall Configuration Information.....	76
4.2	Network devices	80
4.2.1	DeltaV/DMZ perimeter security device	80
4.2.2	DeltaV Smart Switches	81
4.2.2.1	Capabilities and operation	82
4.2.2.2	Management.....	82
4.2.3	DeltaV Firewall-IPD	83
4.2.3.1	Capabilities and operation	83
4.2.3.2	Management.....	84
4.2.3.3	DeltaV SIS Unlock Command Protection	84
4.3	DeltaV workstations and servers.....	86
4.3.1	Workstation and server use	86
4.3.2	Workstation applications and services	86
4.3.2.1	Disabled services.....	86

4.3.2.2	Email	87
4.3.2.3	Internet Explorer	87
4.3.3	Physical security	88
4.3.4	Workstation security templates	89
4.3.5	Workstation locking.....	89
4.3.6	File system.....	89
4.3.7	Removable devices	89
4.3.8	Antivirus software	90
4.3.9	Application Whitelisting.....	91
4.3.10	Network Security Monitor.....	91
4.3.11	Security Information and Event Management	92
4.3.12	Workstation Data, Alarms, and Events	93
4.3.12.1	Acknowledgement to Operator	93
4.3.12.2	Logging alarms	93
4.3.12.2.1	Data historians.....	93
4.3.13	Portable device security.....	94
4.3.14	Microsoft Credential Guard and Device Guard.....	95
4.4	Controllers	96
4.4.1	Physical security	96
4.4.2	Connection to the DeltaV ACN	97
4.4.3	DeltaV Controller I/O protection.....	97
4.4.4	Standalone PK Controller	99
4.5	WirelessHART devices	101
5	Software patching	102
5.1	General patching policy	102
5.1.1	Operational impacts.....	103
5.1.2	Patch list management	105
5.1.3	Patching timeliness.....	106
5.1.4	Patching policies and procedures.....	107
5.2	Microsoft Windows updates.....	108
5.2.1	Introduction	108
5.2.2	Windows non-security updates.....	109
5.2.3	Security updates	109
5.3	DeltaV Hotfixes.....	110
6	Backup and recovery	111

6.1	Overview	111
6.2	Backup/Recovery capability	112
6.3	Backup strategy	112
7	Cybersecurity services	114
7.1	Service standards, policies and procedures	115
7.2	Confidentiality agreements	115
7.3	Standards committees	115
7.4	Security contact	115
7.5	System change procedures	116
7.6	Incident Response Policies and Procedures	116
7.7	System hardening	116
7.8	Conducting cybersecurity risk assessments	117
7.9	Use of troubleshooting tools	117
7.10	Secure disposal guidelines	118
7.11	Incident Response and Program Development Services	118
7.11.1	Incident Response Services	118
7.11.2	Program Development Services	119
8	Final considerations	121