

DeltaV™ Security Manual

Implementing Security on DeltaV Distributed Control Systems



To protect this information this public version only provides the Table of Content information.

A full copy of this document will be provided upon request to your local PSS sales/support office.

For internal Emerson personnel: This document is available on the Global Sales Portal.

This manual is Emerson confidential and intended for use only by customers, employees, LBPs, and others who are responsible for providing security services to Emerson systems and products. It may be provided to potential customers as required to evaluate DeltaV security implementation. It does not require an NDA for distribution.

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

Table of Contents

1	Introduction	1
1.1	Purpose	1
1.2	Organization	2
1.3	Standards	2
1.3.1	Vendor compliance to the published security standards	2
1.3.2	IEC 62443 / ISA99 security standards.....	2
1.4	Relevant documentation.....	3
1.4.1	Background reading.....	3
1.4.2	DeltaV documentation	3
1.4.3	Microsoft documentation.....	4
1.4.4	Third-party product documentation.....	4
1.5	Security and DeltaV system projects.....	5
1.6	Security Collaboration between IT and Operations Departments.....	5
1.7	Submitting Material for This Manual	7
1.8	Glossary.....	8
2	Security basics	9
2.1	Threats to control systems	9
2.2	Assets and compromises	9
2.3	Vulnerabilities	10
2.4	Control system architecture.....	10
2.5	Security policies and procedures.....	12
2.6	Defense-in-depth	13
2.7	Performing risk assessments	13
2.8	Security Hardening	14
3	DeltaV defense-in-depth strategy	15
3.1	Overview.....	15
3.2	Deployment security environment expected for DeltaV systems.....	16
3.3	Physical security.....	18
3.4	Network topology.....	19
3.4.1	Network architecture.....	19
3.4.2	Access from the DMZ	21
3.4.3	DeltaV 2.5 Network.....	21
3.4.4	DeltaV Remote Network	22

3.4.5	DeltaV Inter-Zone Network	24
3.4.6	DeltaV Area Control Network (ACN)	25
3.4.6.1	Description	25
3.4.6.2	Connecting non-DeltaV computers to the ACN	27
3.4.6.3	Extending the ACN using wireless Ethernet bridges	27
3.4.7	DeltaV SIS Networks	28
3.4.7.1	DeltaV SIS with Smart Logic Solvers (SLS1508)	29
3.4.7.2	DeltaV SIS with Electronic Marshalling	29
3.4.8	DeltaV Virtualization Networks	31
3.4.9	Active Directory Design for DeltaV	32
3.4.10	<i>WirelessHART</i> segments.....	34
3.4.10.1	Description	34
3.5	Communications security	36
3.6	User account security	37
3.6.1	Account management.....	37
3.6.1.1	Centralized management of accounts	37
3.6.1.2	Account creation and maintenance	38
3.6.1.3	Operating system and account use	40
3.6.1.4	DeltaV account use.....	40
3.6.1.5	Account expiration	41
3.6.1.6	Removal of temporary accounts	41
3.6.1.7	Removal of unused accounts	42
3.6.2	Passwords	42
3.6.2.1	Complexity	42
3.6.2.2	Default passwords	42
3.6.2.3	Expiration period.....	43
3.6.2.4	Expiration prompt.....	43
3.6.2.5	Reuse.....	43
3.6.2.6	Password policy summary	43
3.6.3	Shared accounts.....	44
3.6.4	Installation-generated user accounts.....	44
3.6.5	Account activity logging	45
3.6.6	Logging into the DeltaV system.....	45
3.7	Device hardening.....	45
3.8	Security event handling	47

3.8.1	Event logging and reporting.....	47
3.8.1.1	General security event handling	47
3.8.1.2	User activities	47
3.8.1.3	Log of security events.....	48
3.8.1.4	Backup Activity Logging.....	48
3.8.2	Event monitoring.....	48
4	DeltaV defense-in-depth components.....	49
4.1	External remote access applications	49
4.1.1	Overview	49
4.1.2	Security requirements specific to remote user access	50
4.1.3	Microsoft Remote Desktop	52
4.1.4	DeltaV remotely accessible applications	53
4.1.5	Emerson Smart Firewall Configuration Information.....	54
4.1.6	Secure remote connection based on Cisco Identify Services Engine (ISE).....	58
4.2	Network devices	60
4.2.1	DeltaV/DMZ perimeter security device	60
4.2.2	DeltaV Smart Switches	61
4.2.2.1	Capabilities and operation	61
4.2.2.2	Management.....	61
4.2.3	DeltaV Controller Firewall.....	62
4.2.3.1	Capabilities and operation	63
4.2.3.2	Management.....	63
4.2.4	DeltaV SIS Intrusion Protection Device (SIS IPD).....	63
4.2.4.1	Management.....	65
4.3	DeltaV workstations and servers.....	65
4.3.1	Workstation and server use.....	65
4.3.2	Workstation applications and services	65
4.3.2.1	Disabled services.....	65
4.3.2.2	Email.....	68
4.3.2.3	Internet Explorer	69
4.3.3	Physical security	69
4.3.4	Workstation security templates.....	70
4.3.5	Workstation locking.....	70
4.3.6	File system.....	70
4.3.7	Removable devices	71

4.3.8	Antivirus software	71
4.3.9	Application Whitelisting.....	72
4.3.10	Network Security Monitoring.....	72
4.3.11	Security Information and Event Management	73
4.3.12	Workstation Data, Alarms, and Events	74
4.3.12.1	Data access	74
4.3.12.1.1	Control parameters.....	74
4.3.12.1.1.1	Acknowledgement to Operator	74
4.3.12.1.1.2	Logging alarms	74
4.3.12.1.2	Data historians.....	74
4.3.13	Portable device security.....	75
4.4	Controllers	76
4.4.1	Physical security	76
4.4.2	Connection to the DeltaV ACN	77
4.4.3	DeltaV Controller I/O protection.....	77
4.5	WirelessHART devices	78
5	Software patching	79
5.1	General patching policy	79
5.1.1	Operational impacts.....	80
5.1.2	Patch list management	82
5.1.3	Patching timeliness.....	83
5.1.4	Patching policies and procedures.....	84
5.2	Microsoft Windows updates.....	85
5.2.1	Introduction	85
5.2.2	Windows non-security updates.....	85
5.2.3	Security updates	86
5.3	DeltaV workstation hotfixes	86
5.4	DeltaV Controller and I/O hotfixes.....	87
6	Backup and recovery	88
6.1	Overview.....	88
6.2	Backup/Recovery capability	89
6.3	Backup strategy.....	89
7	Cybersecurity services.....	90
7.1	Service standards, policies and procedures.....	91
7.2	Confidentiality agreements	91

7.3	Standards committees	91
7.4	Security contact	91
7.5	System change procedures	92
7.6	Incident Response Policies and Procedures	92
7.7	System hardening	92
7.8	Conducting cybersecurity risk assessments	93
7.9	Use of troubleshooting tools	93
8	Final considerations	95