

# ISA-TR99.00.01-2004, Security Technologies for Manufacturing and Control Systems

## Table of Contents

1	Scope
2	Purpose
3	General Terms and Definitions
4	Overview
5	Authentication and Authorization Technologies
5.1	Role-Based Authorization Tools
5.2	Password Authentication
5.3	Challenge/Response Authentication
5.4	Physical/Token Authentication
5.5	Smart Card Authentication
5.6	Biometric Authentication
5.7	Location-Based Authentication
5.8	Password Distribution and Management Technologies
5.9	Device-to-Device Authentication
6	Filtering/Blocking/Access Control Technologies
6.1	Dedicated Firewalls
6.2	Host-based Firewalls
6.3	Virtual Local Area Networks (VLANs)
7	Encryption Technologies and Data Validation
7.1	Symmetric (Secret) Key Encryption
7.2	Public Key Encryption and Key Distribution
7.3	Private Key Signatures and Digital Certificates
7.4	Virtual Private Networks (VPNs)
8	Audit, Measurement, Monitoring, and Detection Tools
8.1	Log Auditing Utilities
8.2	Virus/Malicious Code Detection
8.3	Intrusion Detection Systems
8.4	Network Vulnerability Scanners
8.5	Network Forensics and Analysis Tools (NFAT)
8.6	Host Configuration Management Tools
8.7	Automated Software Management Tools
9	Computer Software
9.1	Server and Workstation Operating Systems
9.2	Real-time and Embedded Operating Systems
9.3	Web and Internet Technologies
10	Physical Security Controls
10.1	Physical Protection
10.2	Personnel Security