S7comm Protocol

Siemens S7 communication protocol for SIMATIC PLCs

OT Security Learning Series

Document 207 | January 2026

Contributors: Matthias Niedermaier

Created with AI assistance

LEARNING RESOURCE

Contents

1 Introduction

Information

S7comm is Siemens' proprietary protocol for communication with SIMATIC S7 PLCs. It is one of the most widely deployed PLC protocols globally and was the primary target of the Stuxnet malware.

Key characteristics:

- Proprietary Siemens protocol
- Used by S7-300, S7-400, S7-1200, S7-1500 PLCs
- Runs over ISO-TSAP (TCP port 102)
- Provides read/write access to PLC memory
- Supports program upload/download

Critical

S7comm was the protocol exploited by Stuxnet to reprogram PLCs controlling uranium enrichment centrifuges. Understanding S7comm security is essential for protecting Siemens-based industrial systems.

2 Protocol Versions

2.1 S7comm vs S7comm-Plus

Aspect	S7comm	S7comm-Plus
PLCs	S7-300, S7-400	S7-1200, S7-1500
Security	None	Optional encryption/auth
Complexity	Simpler	More complex
Documentation	Reverse-engineered	Partially documented

Table 1: S7comm Protocol Versions

2.2 Protocol Stack

3 Network Communication

3.1 Connection Establishment

1. TCP connection to port 102
2. COTP Connection Request (CR)
3. COTP Connection Confirm (CC)

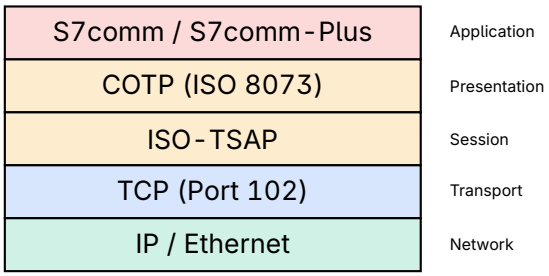

Figure 1: S7comm Protocol Stack

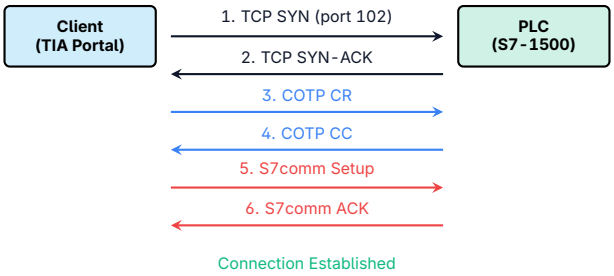

Figure 2: S7comm Connection Establishment

4. S7comm Setup Communication
5. S7comm communication established

3.2 TSAP Addressing

Connections use TSAP (Transport Service Access Point) addresses:

- **Local TSAP** – Client identifier
- **Remote TSAP** – Identifies rack/slot (e.g., 0x0102 = rack 0, slot 2)

Remote TSAP	Target
0x0100	Programming access
0x0102	Rack 0, Slot 2 (typical CPU)
0x0103	Rack 0, Slot 3
0x0200	Rack 1, Slot 0

Table 2: Common TSAP Addresses

4 S7comm Functions

4.1 Function Codes

4.2 Memory Areas

S7comm can access various PLC memory areas:

- **I (Inputs)** – Physical input states

Code	Function	Risk
0x04	Read Variable	Information disclosure
0x05	Write Variable	Process manipulation
0x1A	Request Download	Code injection
0x1B	Download Block	Code injection
0x1C	Download Ended	Code injection
0x1D	Start Upload	Code theft
0x1E	Upload	Code theft
0x28	PLC Control	Start/stop PLC
0x29	PLC Stop	Denial of service

Table 3: S7comm Function Codes and Security Risks

- **Q (Outputs)** – Physical output states
- **M (Markers)** – Internal memory bits
- **DB (Data Blocks)** – Structured data storage
- **T (Timers)** – Timer values
- **C (Counters)** – Counter values

5 Security Vulnerabilities

Critical

Classic S7comm (S7-300/400) has no authentication whatsoever. Anyone with network access can read memory, write values, upload/download programs, and stop the PLC.

5.1 Protocol Weaknesses

- **No authentication** – Connections accepted from any client
- **No encryption** – All traffic in plaintext
- **No integrity** – Messages can be modified
- **Password weakness** – CPU passwords easily bypassed
- **Full access** – Read/write any memory area
- **Program transfer** – Upload/download without verification

5.2 CPU Password Limitations

S7-300/400 CPU passwords:

- Only 8 characters maximum

- Stored in plaintext in project files
- Can be read via S7comm in some cases
- Bypass possible through various techniques
- Provides false sense of security

5.3 Attack Vectors

- **Memory read** – Extract process data, recipes, IP
- **Memory write** – Manipulate setpoints, outputs
- **Program theft** – Upload and reverse-engineer logic
- **Logic injection** – Download malicious program
- **PLC stop** – Halt production
- **Stuxnet-style** – Modify logic while hiding changes

6 Stuxnet and S7comm

Warning

Stuxnet demonstrated the devastating potential of S7comm attacks, causing physical destruction of Iranian uranium enrichment centrifuges by manipulating PLC logic.

6.1 Stuxnet Techniques

- Targeted specific S7-315 and S7-417 PLCs
- Intercepted and modified OB1 (main program block)
- Injected malicious code into OB35 (timed interrupt)
- Hid changes from engineering software
- Manipulated frequency converter outputs
- Caused centrifuge over/under-speed damage

7 S7comm-Plus Security

7.1 S7-1200/1500 Improvements

Newer PLCs offer security features:

- **Access protection levels** – Configurable read/write restrictions
- **Know-how protection** – Block encryption
- **Copy protection** – Bind program to specific CPU
- **TLS option** – Encrypted communication (TIA Portal V17+)
- **Integrity protection** – Digital signatures for programs

7.2 Access Protection Levels

Level	Protection
No protection	Full access (default)
Write protection	Read allowed, write requires password
Read/Write protection	Password required for both
Full protection	No HMI access, password for everything

Table 4: S7-1500 Access Protection Levels

Warning

Even with S7-1500 security features, many deployments use default settings with no protection enabled. Always verify security configuration.

8 Security Mitigations

8.1 Network Controls

Key Point

Given S7comm's lack of native security (especially on S7-300/400), network-level protection is essential.

- **Firewall port 102** – Block from unauthorized networks
- **Network segmentation** – Isolate PLCs in dedicated VLAN
- **Access lists** – Limit which IPs can connect to PLCs
- **Industrial firewall** – S7comm-aware deep packet inspection

8.2 PLC Configuration

- Enable access protection (S7-1200/1500)
- Use strong passwords (where supported)
- Enable know-how protection for sensitive blocks
- Restrict PUT/GET communication

- Disable unused communication functions

8.3 Monitoring

- Log all connections to port 102
- Alert on download/upload operations
- Detect PLC stop commands
- Monitor for connections from new sources
- Compare running program against baseline

9 Tools and Detection

9.1 Analysis Tools

- **Wireshark** – S7comm dissector built-in
- **Snap7** – Open-source S7comm library
- **PLCScan** – Siemens PLC scanner
- **Metasploit** – S7comm auxiliary modules

9.2 Detection Signatures

Monitor for:

- COTP CR packets to port 102
- S7comm function codes 0x1A-0x1E (download/upload)
- S7comm function code 0x29 (stop)
- Unusual TSAP addressing patterns
- High-frequency read/write operations

10 Summary

Key Takeaways

- **Siemens protocol** – Primary for S7 PLC family
- **TCP port 102** – Via ISO-TSAP/COTP
- **Stuxnet target** – Proven attack surface
- **No security (S7-300/400)** – Full unauthenticated access
- **S7comm-Plus** – Improved security options
- **Enable protection** – Configure access levels on S7-1500
- **Network isolation** – Critical for older PLCs

11 Further Reading

Resources

- **Siemens Industrial Security**
  https://www.siemens.com/global/en/products/automation/topic-areas/industrial-security.html
- **CISA – Siemens Advisories**
  https://www.cisa.gov/topics/industrial-control-systems

Research

- **Langner – Stuxnet Analysis**
  https://www.langner.com/
- **Snap7 Project**
  https://snap7.sourceforge.net/

Part of the OT Security Learning Series