TRITON / TRISIS

The First Cyber Attack Targeting Safety Instrumented Systems

OT Security Learning Series

Document 412 | January 2026

Contributors: Matthias Niedermaier

Created with AI assistance

LEARNING RESOURCE

Contents

1 Introduction

TRITON (also known as TRISIS or HatMan) is malware discovered in 2017 that specifically targeted Safety Instrumented Systems (SIS). This attack crossed a critical line—targeting systems designed to prevent catastrophic accidents and protect human life.

Critical

TRITON is the first known malware designed to attack safety systems. By targeting the last line of defense against industrial disasters, the attackers demonstrated willingness to potentially cause loss of life.

1.1 Key Facts

Attribute	Details
Discovery Date	December 2017
Target	Middle Eastern petrochemical facility
Target Systems	Schneider Electric Triconex SIS controllers
Attack Goal	Disable safety systems to enable physical damage
Outcome	Attack failed; SIS triggered safe shutdown
Attribution	Russian government research institute (CNIIHM)

2 Understanding Safety Instrumented Systems

2.1 What is a SIS?

Safety Instrumented System (SIS)

A SIS is an autonomous control system designed to bring a process to a safe state when predetermined conditions are violated. It operates independently from the basic process control system (BPCS) and serves as the last automated line of defense against hazardous events.

SIS Functions

- **Emergency Shutdown (ESD):** Stop processes when dangerous conditions detected
- **Fire & Gas Detection:** Trigger alarms and protective actions
- **Burner Management:** Safe startup/shutdown of fired equipment
- **High Integrity Pressure Protection (HIPPS):** Prevent overpressure

2.2 Defense in Depth Model

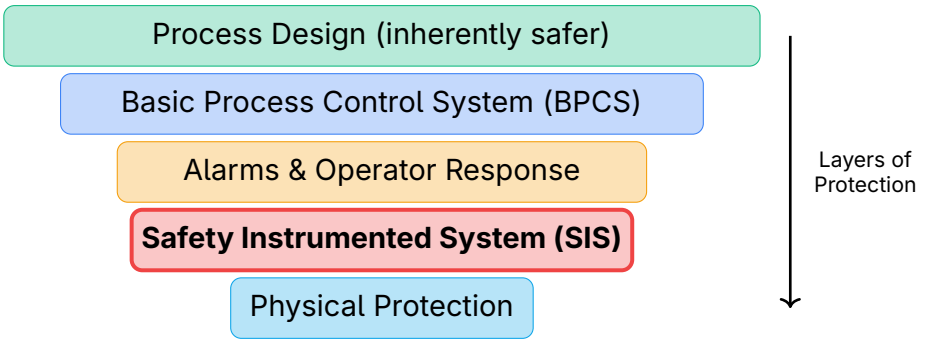

Figure 1: Industrial Defense in Depth – TRITON Targeted the SIS Layer

Warning

The SIS is the last automated barrier before physical protection devices (relief valves, rupture discs) and potential disaster. Compromising a SIS could allow dangerous conditions to escalate unchecked.

3 Attack Analysis

3.1 Attack Timeline

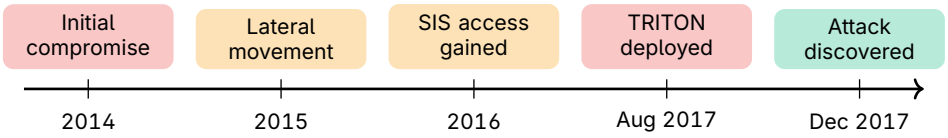

Figure 2: TRITON Attack Timeline

- **2014 (estimated):** Initial compromise of corporate network
- **2014–2017:** Lateral movement and reconnaissance
- **Mid-2017:** Access to SIS engineering workstation gained
- **August 2017:** First TRITON deployment attempt
- **August 2017:** SIS detected invalid code, triggered shutdown
- **December 2017:** Incident publicly disclosed by Dragos and FireEye

3.2 Attack Chain

TRITON Attack Sequence

1. **Initial Access:** Compromised corporate IT network (method unknown)
2. **Lateral Movement:** Pivoted through networks to reach OT
3. **Workstation Compromise:** Gained access to SIS engineering workstation
4. **Reconnaissance:** Studied Triconex controller architecture
5. **Payload Development:** Created custom framework for Triconex
6. **Deployment:** Uploaded malicious code to safety controllers
7. **Failure:** Code error triggered SIS safe shutdown

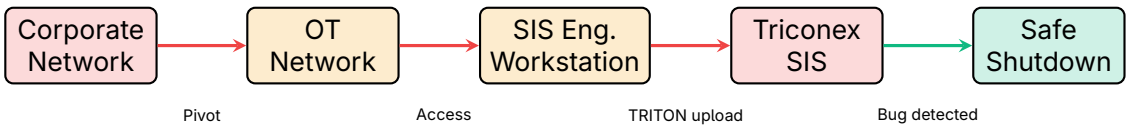

Figure 3: TRITON Attack Path – Attack Failed Due to Code Bug

3.3 Technical Details

TRITON Malware Components

- **trilog.exe:** Main executable disguised as legitimate Triconex software
- **library.zip:** Python libraries compiled for execution
- **inject.bin:** Shellcode payload for Triconex controller
- **imain.bin:** Main malicious logic for the controller

The malware was designed to:

1. Communicate with Triconex controllers using the TriStation protocol
2. Read and write controller memory
3. Upload and execute custom code on the safety controller
4. Potentially disable safety functions while hiding from operators

3.4 Why the Attack Failed

Tip

The attack was discovered because the malicious code contained a bug that caused the safety controller to detect an invalid state and initiate a safe shutdown. This triggered an investigation that uncovered the intrusion.

The SIS performed its designed function—when it detected something wrong, it failed safely. This highlights the importance of defense-in-depth and proper safety system design.

4 Implications

4.1 Crossing the Line

Critical

TRITON represents a significant escalation in cyber attacks:

- First malware to target safety systems specifically
- Demonstrates intent to cause physical harm or death
- Shows advanced understanding of industrial safety architecture
- Required significant investment and specialized expertise

4.2 Potential Consequences

Had the attack succeeded, potential outcomes could have included:

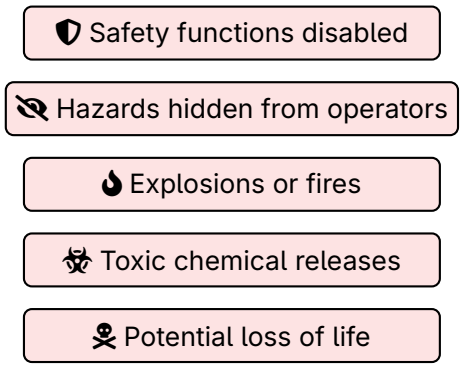

Figure 4: Potential Impact Had TRITON Succeeded

- **Disabled safety functions:** Process could exceed safe limits
- **Masked hazardous conditions:** Operators unaware of danger
- **Explosions or fires:** Uncontrolled chemical reactions
- **Toxic releases:** Environmental contamination
- **Loss of life:** Worker and potentially community casualties

4.3 Attribution

Information

FireEye attributed TRITON to the Central Scientific Research Institute of Chemistry and Mechanics (CNIIHM), a Russian government research institution. This attribution is based on:

- IP addresses traced to CNIIHM
- Testing activity observed from Russian systems
- Technical artifacts in the malware code

5 Lessons Learned

5.1 Defense Recommendations

Key Point

Key security measures for safety systems:

1. **Isolate SIS networks:** Physical or strong logical separation from BPCS
2. **Restrict engineering access:** Limit who can program safety controllers
3. **Monitor SIS changes:** Detect unauthorized modifications to logic
4. **Use hardware key switches:** Physical controls for programming mode
5. **Implement change management:** Document and approve all SIS changes
6. **Regular integrity checks:** Verify SIS logic against approved baseline

5.2 Network Architecture

Warning

SIS engineering workstations should not be connected to general OT networks. Access to safety system programming should require physical presence and multiple authorization steps.

Recommended architecture:

- Separate network segment for SIS
- Dedicated, hardened engineering workstations
- No direct connectivity between SIS and business networks
- Physical key switches to enable programming mode
- Multi-person authorization for safety logic changes

5.3 Industry Response

TRITON prompted significant industry action:

- Schneider Electric released security advisories and patches
- ICS-CERT issued alerts and recommended mitigations
- Industry groups developed SIS-specific security guidelines
- Increased focus on safety system cybersecurity in standards

6 Detection and Response

6.1 Indicators of Compromise

- Unauthorized TriStation protocol communications
- Unexpected files on SIS engineering workstations
- Safety controller in programming mode unexpectedly
- Anomalous network traffic to/from safety systems
- Unexpected safety system shutdowns

6.2 Monitoring Recommendations

- **Network monitoring:** Detect unauthorized SIS communications
- **File integrity:** Monitor engineering workstations for changes
- **Access logging:** Track who accesses SIS programming tools
- **Configuration baselines:** Compare SIS logic against known-good
- **Physical controls:** Monitor key switch positions

7 Further Reading

Technical Reports

- **Dragos** – TRISIS Malware Analysis
  https://www.dragos.com/resources/whitepaper/trisis-analyzing-safety-system-targeting-malware/
- **FireEye / Mandiant** – TRITON Attribution Report
  https://www.mandiant.com/resources/reports
- **Schneider Electric** – Security Notification
  https://www.se.com/ww/en/work/support/cybersecurity/security-notifications.jsp

Government Resources

- **CISA** – MAR-17-352-01 HatMan/TRITON
  https://www.cisa.gov/news-events/analysis-reports
- **NIST** – Cybersecurity Framework
  https://www.nist.gov/cyberframework

Standards

- **IEC 61511** – Functional Safety: Safety Instrumented Systems for the Process Industry
- **ISA/IEC 62443** – Industrial Automation and Control Systems Security

Part of the OT Security Learning Series