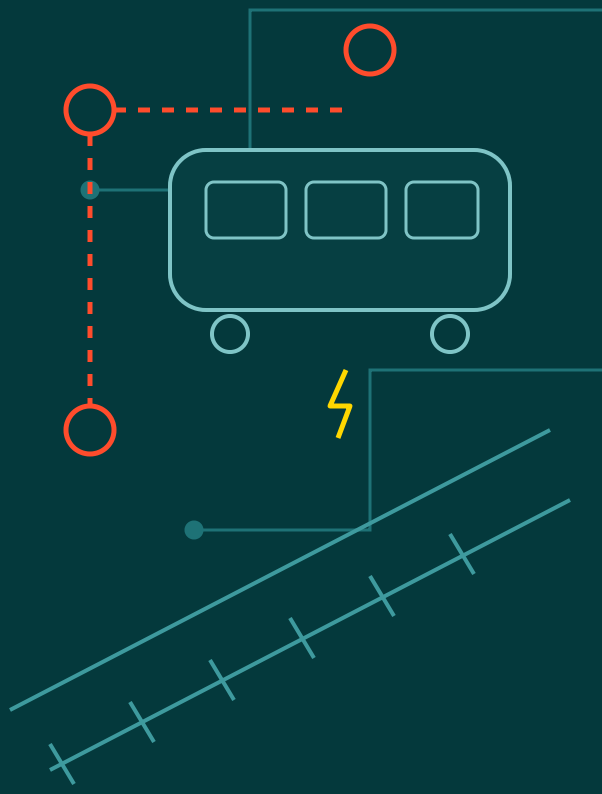
CASE STUDY

CS-2026-07

ioSENTRIX

Your Trusted Partner in Cybersecurity



INDUSTRIAL CONTROL SYSTEM SECURITY

How one exposed network segment led to a simulated train-control outage

A test of a communication-based train control system crossed segmented networks to the nodes that run train communications.

CLIENT	SERVICE	FINDINGS	VERIFIED
Passenger rail operator	ICS and network penetration testing	35+, including 4 Critical	**Fixes re-assessed by ioSENTRIX**

AT A GLANCE

CLIENT
Passenger rail operator

SYSTEM
Communication-based train control (CBTC) in service for several years

SERVICE
ICS, IoT and IIoT penetration testing

SCOPE
Segmented networks, proprietary equipment and several ICS systems

ENVIRONMENT
Lab replica of production, without live trains

ENGAGEMENT
A multi-week engagement

VERIFIED
Fixes re-assessed by ioSENTRIX

TESTED BY
ioSENTRIX ICS and network testers

EXECUTIVE SUMMARY

From an exposed segment to the nodes that control train communications

A passenger rail operator asked ioSENTRIX to test the security of its communication-based train control system. A successful attack could stop operations for days and put passengers at risk.

Starting from one exposed network segment, our testers pivoted across segmented networks to the nodes that control train communications, and simulated shutdowns that caused an outage across operating regions in the lab. The client fixed the findings and ioSENTRIX re-assessed them.

1	35+	0
exposed network segment was enough to start	findings, 4 of them Critical	live trains touched: every test ran in a lab replica

Built to fail safe, the system had not been built to keep an attacker out.

Details in this case study are anonymised and generalised. Methods that could harm other products are withheld.

© 2026 ioSENTRIX LLC

01 What we found

THEME · NETWORK FINDING 1

Unpatched bridging nodes let testers cross segments

The nodes that connected several segments ran unpatched Windows, left unpatched because the network was air-gapped. From an exposed segment, our testers compromised those nodes, then pivoted from them into other segmented networks.

Business impact: segmentation slowed an attacker down but did not stop one from reaching operational systems.

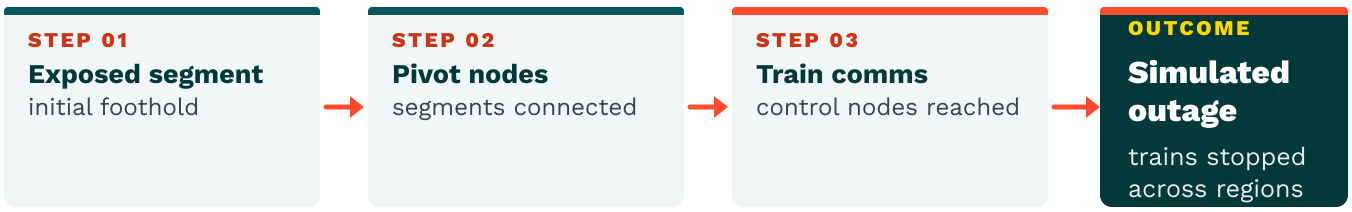
THEME · ICS FINDING 2

Train communication nodes could be reached and shut down

Our testers gained access to sensitive nodes that control train system communication. In the lab replica, simulated shutdowns of several trains produced an outage across different operating regions.

Business impact: an attack of this kind could halt service, cost days of downtime and put passenger safety at risk.

Figure 1. One chain from an exposed segment to a simulated multi-region outage



HOW WE FOUND IT

There are no open testing standards for much proprietary rail and ICS software, so there was nothing for a scanner to check against. Finding this took learning how the equipment works and testing it by hand in a production-like lab.

© 2026 ioSENTRIX LLC

02 Results

Figure 2. Findings by severity (35+ findings)



Figure 3. What changed in the train control environment — **Fixes re-assessed by ioSENTRIX**

AREA	BEFORE THE TEST	AFTER REMEDIATION
Segmentation	Unpatched Windows on bridging nodes allowed pivoting between segments	● Fixes implemented by the operator's technical staff
Train communications	Control nodes were reachable; simulated shutdowns caused a multi-region outage in the lab	● Fixes implemented, then re-assessed by ioSENTRIX
Incident response	The plan did not account for these attack paths	● The new threats were added to the incident response plan

03 Lessons for operators of industrial systems

Air-gapped is not patched

The nodes bridging segments ran unpatched Windows because the network was air-gapped. Isolation delayed patching; it did not remove the risk.

Finding 1 · NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security

Test hard, in a faithful lab

A replica of production let our testers push all the way to a simulated outage without touching a live train.

Approach

Fail-safe is not cyber-safe

Safety engineering assumes faults, not attackers. Add attack scenarios like these to incident response, as this operator did.

Finding 2

ioSENTRIX

Running operational technology? See a sample ICS test report or book a strategy session.

iosentrix.com/contact-us

contact@iosentrix.com

+1 (888) 958-0554

13800 Coppermine Rd, Suite 190
Herndon, VA 20171

CREST-accredited · ISO/IEC 27001 certified · SOC 2 Type 2 attested

© 2026 ioSENTRIX LLC. General information only. Client details anonymised.