ELECTRIC GRID USE CASE

Modified Relay Settings After Vendor Maintenance

An electric grid use case showing how REMI turns event logs and source records into a cyber SITREP with confirmed findings, unresolved questions, and immediate next steps.

At 6:22 AM, the protection engineering lead at North Valley Electric noticed that the feeder protection profile for **BRK-17** did not match the approved post-maintenance baseline. The relay was online, but the pattern was wrong: **SEL-451-2F** showed a new active settings group, the upload timestamp came after the approved vendor window, and the breaker event record did not line up with the signed relay-setting package.

The engineering lead reported it to the utility's IT manager, who reviewed the relay engineering workstation and found activity from **vendor_relay_03** on **ENG-RELAY-02**. The file name matched the work order, **BRK17_Q3_MAINT.set**, but the checksum did not match the approved file hash. Firewall records then showed traffic from **10.42.22.31** toward **SUB-GW-17** before the modified settings package was uploaded to the relay.

That changed the concern from vendor maintenance review to adversarial relay manipulation. The warning signs were connected behaviors: an approved-looking relay file, a checksum mismatch, vendor-account activity, engineering workstation access, substation gateway traffic, and relay settings that changed after the authorized maintenance window closed.

Investigator Arrives Onsite

Later that morning, the investigator arrives onsite at **North Valley Electric Operations Center**. The investigator speaks with the protection engineering lead who noticed the relay-setting mismatch, the utility IT manager who reviewed the engineering workstation, the substation engineer responsible for **SUB-GW-17**, and the vendor coordinator responsible for the maintenance package.

After those conversations, the investigator requests copies of the available event logs and source records so they can be analyzed in REMI. The goal is to determine how the vendor account, relay settings file, checksum mismatch, engineering workstation, substation gateway, and relay upload fit together as an adversarial cyber operation. The more complete the log package is, the wider the investigative coverage becomes.

Event Logs to Request

- **Relay setting files and hashes** showing approved baseline, uploaded file, checksum, active settings group, and package history.
- **Relay event and sequence-of-events logs** showing upload time, setting group activation, breaker events, and device responses.
- **Engineering workstation telemetry** showing file access, relay software activity, command shells, scripts, and process execution.
- **Vendor access and identity records** showing account use, session timing, MFA approval, assigned technician, and privilege changes.
- **Firewall and OT network flow logs** showing traffic between engineering workstations, jump hosts, substation gateways, and relay networks.
- **SCADA, EMS, historian, and alarm records** showing breaker status, relay communication, alarms, acknowledgements, and time-aligned operating changes.
- **Vendor work orders, relay-setting tickets, maintenance records, and asset-owner approvals** showing whether the upload matched authorized work.

REMI Flagged

- **Relay setting upload** to **SEL-451-2F** after the authorized maintenance window.
- **Approved-looking settings file** named **BRK17_Q3_MAINT.set** tied to the work order.
- **Checksum mismatch** between the uploaded settings file and the approved relay package.
- **Vendor-account activity** involving **vendor_relay_03** on **ENG-RELAY-02**.
- **Traffic toward substation gateway SUB-GW-17** from **10.42.22.31** before the upload.
- **Shared evidence links** across account, file name, checksum, workstation, gateway, relay event, and maintenance records.

Correlation and SITREP Output

The raw logs are imported into REMI for analysis. REMI identifies the flagged behaviors inside the evidence package, then correlates records that share the same account, relay file, checksum, workstation, substation gateway, relay event, SCADA record, and operational timestamp.

REMI Correlated

- **Vendor account and engineering workstation** linked through **vendor_relay_03**, **ENG-RELAY-02**, and the relay maintenance window.
- **Settings file and checksum mismatch** linked through **BRK17_Q3_MAINT.set**, approved baseline records, and uploaded package metadata.
- **Workstation traffic and substation gateway** linked from **10.42.22.31** to **SUB-GW-17** through firewall and jump-host records.
- **Relay upload and active settings group** linked by timestamp to **SEL-451-2F** and **BRK-17** feeder protection records.
- **Shared evidence path** connecting account, workstation, settings file, checksum, gateway traffic, relay event, SCADA status, and maintenance records.

SITREP Output Includes

- **Confirmed findings** showing what the evidence proves.
- **Unresolved questions** showing what still needs confirmation.
- **Additional source data needed** to close specific answer gaps.
- **Questions to ask IT, engineering, vendors, and system owners.**
- **Artifacts to preserve or sandbox** before cleanup.
- **Malware paths, scripts, services, or scheduled tasks to remove** after preservation.
- **Verification steps** to confirm the activity does not return.

How REMI Reconstructs It

The following simulated electric-grid excerpt shows the level of case-specific detail REMI can produce inside a SITREP. Names, accounts, IP addresses, systems, files, and records are examples, but the structure reflects the level of detail REMI is designed to generate from the evidence package.

Modified Relay Settings After Vendor Maintenance

REMI confirmed that **vendor_relay_03** accessed **ENG-RELAY-02** during the relay maintenance window and that **BRK17_Q3_MAINT.set** was uploaded to **SEL-451-2F** after the authorized window closed. The file name matched the work order, but the uploaded checksum did not match the approved relay package.

REMI correlated the **vendor account**, **engineering workstation**, **settings file**, **checksum mismatch**, **substation gateway traffic**, and **relay setting activation** into one evidence path. The activity used an approved-looking maintenance artifact, which kept the individual records quiet until the file hash, timestamp, and relay event were connected.

The SITREP identified confirmed findings, including the **vendor account**, **engineering workstation**, **relay settings file**, **checksum mismatch**, **SUB-GW-17 traffic**, **SEL-451-2F upload**, and **BRK-17 setting group change**. It also identified unresolved questions: who controlled **vendor_relay_03** during the upload window, where the modified settings file was staged, whether additional relay files were altered, and whether the changed protection profile affected other feeders.

REMI generated immediate next steps: preserve **relay setting files**, **approved hashes**, **relay event logs**, **ENG-RELAY-02 EDR telemetry**, **vendor access records**, **firewall flows**, **SCADA records**, and **maintenance tickets**; request the signed relay-setting package and vendor checksum record; compare **SEL-451-2F** against the approved baseline; restrict **vendor_relay_03**; sandbox the modified settings package; restore the approved relay profile after preservation; and verify that breaker protection, relay communication, and SCADA status return to expected behavior.