Title: Line Supervision Test	
Objective: Verify system is installed using acceptable standards and practices, communicates properly, and provides proper protection of assets and meets or exceeds the contract performance specification. Also verifies the ability of a system to recover after a communications failure.	
Applicability: Sensors, Transmission lines, Panels (FDBs and ACUs), Workstations, Servers, IDS, ACS.	

Notes:
1. Procedures are designed assuming a system consisting of an Access Control Unit (ACU) (for example a door controller) with associated devices that is connected to a workstation.
2. The field technician may need keys to access components in locked rooms for these tests.
3. A detailed link testing list is essential to ensuring 100% system testing.
4. The purpose of alarm annunciation is to provide a correct and useful location of the alarm.
5. Real-time voice communications between the workstation operator and the field technician is required.
6. Verify that alarms annunciate quickly and meet appropriate standards.

Steps	Actions	Expected Results
1.0	**Communications Failure and Access Control Unit (ACU) Test**	
1.1	Disconnect the network communication line at the ACU.	Network communication failure alarm received at the workstation.
1.2	Repeat access, access denied, egress, and alarm (door held or door forced) tests.	Tests results are consistent with the results from the respective tests, but alarms are not received at the workstation.
1.3	Reconnect the communications line.	Workstation receives all system transaction logs and alarms from tests performed while communications were disconnected. Workstation shows communications have been restored.
1.4	Clear the alarms at the workstation.	The active alarm queue is empty.
2.0	**ACU to Credential Verification Device Failure Test**	
2.1	Disconnect the communication line from the ACU to the credential verification device.	Line supervision alarm received at the workstation.
2.2	Repeat Valid Credential test.	Device is unresponsive, door lock does not release.
2.3	Reconnect the communication line from the ACU to the credential verification device.	Line supervision alarm is still active.
2.4	Clear the alarms at the workstation.	The active alarm queue is empty.
2.5	Repeat Valid Credential test.	Transaction logged at the workstation. Door lock releases.
3.0	**Open Circuit Test (conduct this test for each**	

Steps	Actions	Expected Results
	device)	
3.1	Disconnect the device signal lead from the ACU.	Line supervision alarm received at the workstation.
3.2	Reconnect the device signal lead from the ACU.	The alarm is still active.
3.3	Clear the alarms at the workstation.	The active alarm queue is empty.
4.0	**Short Circuit Test (conduct this test for each device)**	
4.1	Place a jumper wire across the terminal blocks for the input and short the device's input wires together.	Line supervision alarm received at the workstation.
4.2	Remove the jumper wire.	The alarm is still active.
4.3	Clear the alarms at the workstation.	The active alarm queue is empty.

Title: Power Failure Test	

Objective: Verify system is installed using acceptable standards and practices, communicates properly, and provides proper protection of assets and meets or exceeds the contract performance specification.	

Applicability: Backup Power, ACS, IDS	

Notes:
1. Procedures are designed assuming a system consisting of an Access Control Unit (ACU) (for example a door controller) with associated devices that is connected to a workstation.
2. Take appropriate safety precautions because this test involves energized power sources.
3. If backup power is batteries, a multi-meter or voltage meter is required to test voltage.
4. Real-time voice communications between the workstation operator and the field technician is required.
5. Perform these tests with the associated zone in the SECURE state.

Steps	Actions	Expected Results
1.0	**AC Power Loss and Restoration Test**	
1.1	Disconnect AC power from the ACU.	AC power failure alarm is received at the workstation. No intrusion alarms are generated from the power loss. System continues to operate correctly.
1.2	Reconnect AC power to the ACU.	Workstation notifies that AC power has been restored. No intrusion alarms are generated from the change in power source. System continues to operate correctly. AC power failure alarm is not cleared until acknowledged at the workstation.
1.3	Clear alarm at workstation.	Active alarm queue is empty.
2.0	**Backup Power Duration Test**	
2.1	Allow the system to run under normal conditions on battery power. Note the time of disconnection from AC power. (If backup power is a battery, measure the voltage of the battery immediately after disconnecting AC power).	System switches to backup power without issues. (If battery backup is used, document the measured voltage.)
2.2	Allow the system to run until at least the required duration has passed. (If backup battery is used, measure the voltage of the battery prior to reconnecting the AC power in the next step).	System operated correctly for the entire required duration. (If battery backup is used, document the measured voltage.)
2.3	Reconnect AC power.	System switches to AC power without issues.
3.0	**Battery Recharge Test (if applicable)**	
3.1	After Backup Power Duration Test has been performed, reconnect AC power and note the time.	System switches to AC power without issues.
3.2	Allow the system to run for the required recharge duration.	System operated correctly for the entire required duration.
3.3	Measure the battery's voltage.	Voltage on the battery has returned to full value as measured in the Backup Power Duration Test.

Title: Tamper Test

Objective: Verify system is installed using acceptable standards and practices, communicates properly, and provides proper protection of assets and meets or exceeds the contract performance specification.

Applicability: Almost all devices and equipment covers; all panels.

Notes:
1. Perform the tamper tests with the associated zone in the ACCESS state.
2. Perform the tamper test on all tampers associated with every device in the system. For example: tampers included in card readers, BMSs, door hardware, and junction boxes.
3. The Tamper Switch Test is for tampers inside the component.
4. The Mounting Tamper Test is for tampers that go between the device and the mounting surface. This test is to be performed if applicable.

Steps	Actions	Expected Results
1.0	**Tamper Switch Test**	
1.1	Gradually remove the cover of the device, junction box, or panel until an alarm occurs.	A tamper alarm is received at the workstation before the tamper switch is accessible and before there is direct line of sight to any internal components.
1.2	Reattach the cover.	
1.3	Clear the tamper alarm at the workstation.	The active alarm queue is empty.
2.0	**Mounting Tamper Test (if applicable)**	
2.1	Attempt to non-destructively remove the device from the mounting surface.	Alarm received at workstation before any components or wiring are visible.
2.2	Reattach the cover.	
2.3	Clear the tamper alarm at the workstation.	The active alarm queue is empty.