Title: Arming/Disarming Keypad Test

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

Applicability: Intrusion Detection System (IDS)

Notes:

1. Assumes a room with an arming/disarming keypad on the secure side, a Balanced Magnetic Switch (BMS) on the door, and motion sensor coverage.
2. Program alarm delays only for those sensors that would activate prior to the user reaching the keypad and entering the disarm code. All other sensors operate without delay.
3. Real-time voice communications between the workstation operator and the field technician is required.

Steps	Actions	Expected Results
1.0	**Arming Test**	
1.1	Ensure the room is in the ACCESS state.	Workstation indicates zone is in ACCESS state.
1.2	Input correct arming code.	No alarms are received at the workstation. Keypad and system both show SECURE.
1.3	Exit within the appropriate delay period.	No alarms are received at the workstation. Zone is SECURE.
2.0	**Disarming Test**	
2.1	Ensure the room is in the SECURE state.	Workstation indicates zone is in SECURE state.
2.2	Enter the secure space.	BMS and motion sensors show activity, but no alarms are received at the workstation.
2.3	Enter the correct disarming code within the delay period.	No alarms are received at the workstation. Keypad and system both show ACCESS.
2.4	Walk through the zone and attempt to activate each sensor that has been disarmed.	No alarms are received at the workstation.
2.5	Attempt to activate 24/7 alarms (such as emergency exits).	Alarm received at workstation.
2.6	Clear the alarm at the workstation.	The active alarm queue is empty.
3.0	**Incorrect Code Test - Arming**	
3.1	Ensure the room is in the ACCESS state.	Workstation indicates zone is in ACCESS state.
3.2	Input an incorrect arming code.	No alarms are received at the workstation. Keypad alerts user that system was not armed. Keypad and system both show ACCESS.
3.3	Repeat 3.2 until the maximum number of allowed attempts is reached.	Alarm received at workstation.
3.4	Clear the alarm at the workstation.	The active alarm queue is empty.

Steps	Actions	Expected Results
4.0	**Incorrect Code Test - Disarming**	
4.1	Enter the secure space.	BMS and motion sensors show activity, but no alarms are received at the workstation.
4.2	Enter an incorrect disarming code.	Keypad alerts user that system did not disarm. Keypad and system both show SECURE.
4.3	Repeat 4.2 until the maximum number of allowed attempts is reached within the allotted time.	Workstation shows keypad alarm.
4.4	Clear the alarm at the workstation.	The active alarm queue is empty.
5.0	**Delayed Exit After Arming Test**	
5.1	Enter the correct arming code.	No alarms are received at the workstation. Keypad and workstation both show SECURE.
5.2	Exit the secure space after the programmed delay period ends.	Intrusion alarm received at the workstation after the alarm is received.
5.3	Clear the alarm at the workstation.	The active alarm queue is empty.
6.0	**Delayed Disarming Test**	
6.1	Enter the armed space.	BMS and motion sensors show activity, but no alarms are received at the workstation.
6.2	Wait for the delay period to end.	Intrusion alarm is received at the workstation.
6.3	Enter the correct disarming code.	Keypad and workstation both show ACCESS. Alarms are still active.
6.4	Clear the alarm at the workstation.	The active alarm queue is empty.
7.0	**Duress Code Test**	
7.1	Ensure the room is in the SECURE state.	Workstation indicates zone is in SECURE state.
7.2	Enter the secure space.	BMS and motion sensors show activity, but no alarms are received at the workstation.
7.3	Enter the duress code within the delay period.	Alarm is received at the workstation. Keypad shows ACCESS.
7.4	Clear the alarm at the workstation.	The active alarm queue is empty.

Title: Magnetic Lock

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: Doors and gates. Magnetic Locks. Electronic Entry Control Systems (EECS). NFPA and life safety codes.

Notes:

1. These procedures are based on interior door with card reader for entrance. This magnetic lock is installed in a fail secure configuration. On the secure side, the door has a magnetic lock with door position switch, PIR REX (Passive Infrared Request to Exit) sensor above the door, and a Push To Exit button on the wall (this is as a backup exit system).
2. All standard access control tests are needed in addition to this test. The intent of this test is to ensure egress due to the dangers of magnetic locks.
3. Ensure that the magnetic lock is installed correctly: it is flush with the closer, is on the handle side of the door, and the closer does not slam the door.
4. Assumes only one credential is required for entry (i.e. card only).
5. The Power Failure – Fail Secure Test is performed if the door is configured in "Fail Secure" mode (i.e. in a power fail situation, the door defaults to the locked condition).
6. Real-time voice communications between the workstation operator and the field technician is required.
7. For Steps 9.0 and 10.0, coordinate testing so that building occupants and emergency response forces along with all appropriate parties understand that testing is occurring.

Steps	Actions	Expected Results
1.0	**Lock Test**	
1.1	Ensure that the door is closed and locked. Contract the operator to verify that the door is secure.	Door is locked and secure.
1.2	Activate the door hardware from the public side and attempt open the door.	Door does not open. No alarm received at the workstation.
2.0	**PIR REX Field of View Test**	
2.1	Stand slightly outside of the PIR's expected field of view	PIR does not detect test subject. Lock does not release.
2.2	Staying slightly outside of the PIR's expected field of view, walk the boundary of the PIR.	PIR does not detect test subject. Lock does not release.
3.0	**Valid Credential Test**	
3.1	Present a valid badge to the reader.	Transaction logged. Lock releases.
3.2	Open door and enter.	Door indicates as open. No alarm is received at workstation.
3.3	Close the door.	Door indicates as closed. No alarm is received at workstation. Lock reactivates when door is closed. The active alarm queue is empty.
4.0	**Invalid Credential Test**	
4.1	Present Invalid Badge to the reader.	An invalid credential alarm is received at the

Steps	Actions	Expected Results
		workstation. Transaction logged. Door lock does not release.
4.2	Clear the alarm at the workstation.	The active alarm queue is empty.
5.0	**Exit Test**	
5.1	Walk up to the door.	PIR releases the magnetic lock.
5.2	Walk through the door.	Door indicates as open at the workstation. Alarm does not activate.
5.3	Close the door.	Door indicates as closed. No alarm is received at workstation. Lock reactivates when door is closed. The active alarm queue is empty.
6.0	**Push-To-Exit Test**	
6.1	Walk up to the door and stand to the side (with hand on the Push To Exit button) until the PIR no longer detects the person trying to exit.	PIR releases the magnetic lock and relocks it after appropriate time. No alarm received.
6.2	Push the Push To Exit button.	Magnetic Lock releases. No alarm received.
6.3	Have person outside the room open the door.	Door opens and indicates as open at the workstation. Alarm is received at workstation.
6.4	Close the door and clear the alarm queue.	Door indicates as closed. Lock reactivates when door is closed. The active alarm queue is empty.
7.0	**Power Failure – Fail Secure Test** (This procedure is for use when lock is configured in the Fail Secure mode. I.e. lock remains active when power fails.)	
7.1	Disconnect AC power from the door controller.	
7.2	Activate the door hardware from the public side and attempt open the door.	Door does not open. No alarm received at the workstation.
7.3	Attempt to exit through the door by means of the PIR REX.	Free egress is achieved.
7.4	Attempt to exit through the door by means of the Push To Exit button. (Stand still on the secure side of the door until the PIR disengages to do this).	Free egress is achieved.
8.0	**Power Failure – Fail Safe Test** (This procedure is for use when lock is configured in the Fail Safe mode. I.e. lock disengages when power fails.)	
8.1	Disconnect AC power from the door controller.	
8.2	Activate the door hardware from the public side and	Door opens. Door forced alarm received at the

Steps	Actions	Expected Results
	attempt open the door.	workstation.
8.3	Attempt to exit through the door from the secure side.	Free egress is achieved.
9.0	**Fire Alarm – Fail Secure Test** (This procedure is for use when lock is tied into the fire alarm system and is configured in the Fail Secure mode. I.e. lock remains active when power fails.)	
9.1	Activate the fire alarm system.	
9.2	Activate the door hardware from the public side and attempt open the door.	Door does not open. No alarm received at the workstation.
9.3	Attempt to exit through the door by means of the PIR REX.	Free egress is achieved.
9.4	Attempt to exit through the door by means of the Push To Exit button. (Stand still on the secure side of the door until the PIR disengages to do this).	Free egress is achieved.
10.0	**Power Failure – Fail Safe Test** (This procedure is for use when lock is tied into the fire alarm system and is configured in the Fail Safe mode. I.e. lock disengages when power fails.)	
10.1	Activate the fire alarm system.	
10.2	Activate the door hardware from the public side and attempt open the door.	Door opens. Door forced alarm received at the workstation.
10.3	Attempt to exit through the door from the secure side.	Free egress is achieved.

Title: Mechanical Turnstile

Objective: Verify device is installed using acceptable standards and practices, communicates properly with the Access Control System (ACS), and provides proper protection of assets and meets or exceeds the contract performance specification.

Applicability: Access control systems. Examples: Perimeter gates, fence lines, remote sites.

Notes:

1. These procedures assume a single-rotor mechanical turnstile with an entry card reader. Exit lane is the same as entry lane, and occupants are allowed free egress.
2. Assumes a single credential required for entry (i.e. card only).
3. Perform valid and invalid credential tests for entry.
4. The cards to be prepared prior to testing and used for these tests are as follows:
   Card 1: Authorized to access all areas.
   Card 2: Time zone restricted card. Valid for only normal duty hours.
   Card 3: Time zone restricted card. Valid for only non-duty hours.
   Card 4: Enrolled user with expired access.
   Card 5: Un-programmed card.
   Card 6: Card with insufficient access permissions.
5. For Valid Credential Tests (Step 2.0), use cards 1 and 2.
6. For Invalid Credential Tests (Step 3.0), use cards 3, 4, 5, and 6.
7. Real-time voice communications between the workstation operator and the field technician is required.
8. Perform these tests with the associated zone in the SECURE state.
9. Line Supervision, Power Fail, and Tamper Tests need to be performed in addition to these procedures.

Steps	Actions	Expected Results
1.0	**Mechanical Test**	
1.1	From the unsecure side, verify that the turnstile rotor assembly is locked. Attempt to enter from the unsecure side without a credential.	Turnstile does not allow access. No alarm received at the workstation.
2.0	**Valid Credential Access Test**	**(It is recommended to repeat this test at least 3 times with no failures to help ensure proper functionality)**
2.1	Present a valid credential to the reader.	Transaction logged at workstation. Turnstile mechanical lock releases and allows rotor assembly to turn.
2.2	Pass through the turnstile.	Turnstile rotor assembly rotates to allow one person to pass through the turnstile and reactivates the mechanical lock.
3.0	**Invalid Credential Access Test**	**(It is recommended to repeat this test at least 3 times with no failures to help ensure proper functionality)**
3.1	Present invalid credential to the reader.	An invalid credential alarm is received at the workstation. Turnstile does not release.
3.2	Clear the alarm at the workstation.	The active alarm queue is empty.
3.3	Repeat for each of the invalid credentials.	

Steps	Actions	Expected Results
4.0	**Egress Test**	**(It is recommended to repeat this test at least 3 times with no failures to help ensure proper functionality)**
4.1	Verify turnstile rotor assembly is locked from the unsecure side.	Turnstile does not allow access. No alarm received at the workstation.
4.2	From the secure side, attempt to egress through the turnstile to the unsecure side.	Turnstile rotates to allow free egress.
4.3	Repeat 4.1 to ensure turnstile rotor assembly lock is active after egress.	Turnstile does not allow access. No alarm received at the workstation.

Title: Single Door with an Electronic Entry Control System (EECS)

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: Electronically Controlled Access Doors. These procedures are based on the system shown in UFC 4-021-02 Figure 3-5.

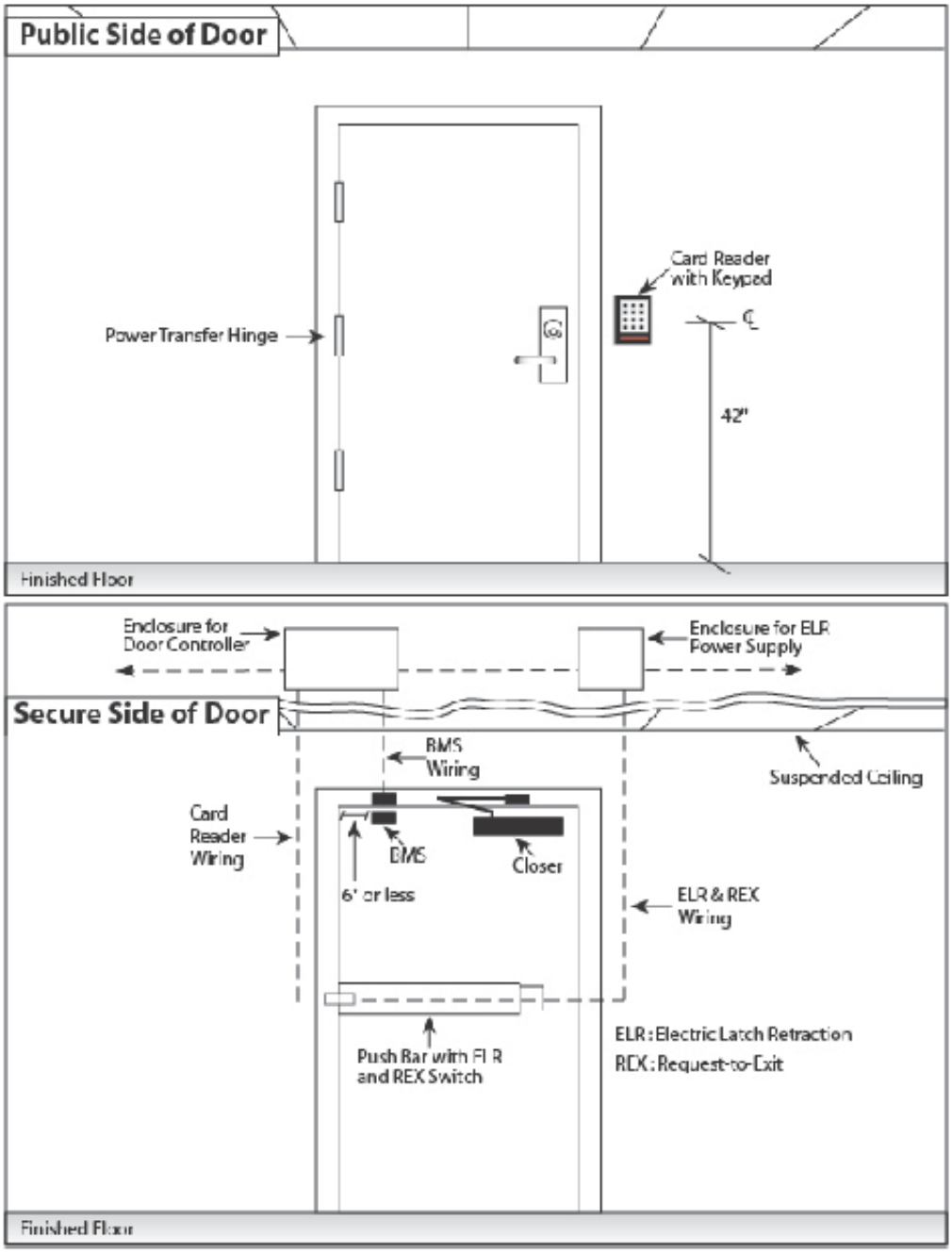
Notes:

1. These procedures are based on the system shown in UFC 4-021-02 Figure 3-5.
2. Assumes 2 credentials required for entry (i.e. card and PIN).
3. The cards to be prepared prior to testing and used for these tests are as follows:
   Card 1: Authorized to access all areas.
   Card 2: Time zone restricted card. Valid for only normal duty hours.
   Card 3: Time zone restricted card. Valid for only non-duty hours.
   Card 4: Enrolled user with expired access.
   Card 5: Un-programmed card.
   Card 6: Card with insufficient access permissions.
4. For Valid Badge Tests (Steps 3.0-5.0), use cards 1 and 2.
5. For Invalid Badge Tests (Step 6.0), use cards 3, 4, 5, and 6.
6. Real-time voice communications between the workstation operator and the field technician is required.
7. Perform these tests with the associated zone in the SECURE state.
8. Line Supervision, Power Fail, and Tamper Tests need to be performed in addition to these procedures.
9. Perform the tamper test on all tampers associated with the ACS portal. For example: tampers included in card readers, BMSs, door hardware, and junction boxes.

Steps	Actions	Expected Results
1.0	**Nuisance Test**	
1.1	Ensure that the door is closed and locked. Contract the operator to verify that the door is secure.	Door is locked and secure.
1.2	Without activating the door hardware, push and pull on the door to attempt to trigger a nuisance alarm.	Door does not open. No alarm received at the workstation.
2.0	**Mechanical Lock Test**	
2.1	Turn the handle and attempt to open the door.	Door does not open. No alarm received at the workstation.
3.0	**Door Forced Test**	
3.1	Either use a manual key override or open the door and fix the latch in the retracted position in such a way that the request to exit switch is not activated. Close the door. Ensure the door is shown as closed at the workstation and that the active alarm queue is empty.	Door closed. Latch retracted. The active alarm queue is empty.
3.2	Slowly open the door until the operator notifies of a door forced alarm.	Door forced alarm received at workstation before door has moved ¼ inch.
3.3	Return the door and all components to normal operating condition and ensure the door is closed.	

Steps	Actions	Expected Results
3.4	Clear the alarm at the workstation.	The active alarm queue is empty.
4.0	**Valid Badge and no PIN Test**	
4.1	Present a valid badge to the reader without entering a PIN.	Transaction logged at the workstation. Door lock does not release.
5.0	**Valid Badge and Correct PIN Test (See note 4)**	
5.1	Present a valid badge to the reader and enter the correct PIN.	Transaction logged at the workstation. Door lock releases.
5.2	Open door and enter.	Door indicates as open. No alarm is received at the workstation.
5.3	Close the door.	Door indicates as closed. Door lock reactivates. No alarm is received at workstation. The active alarm queue is empty.
6.0	**Valid Badge and incorrect PIN Test (See note 4)**	
6.1	Present a valid badge to the reader, and enter an incorrect PIN.	An invalid credential alarm is received at the workstation. Transaction logged. Door lock does not release.
6.2	Clear the alarm at the workstation.	The active alarm queue is empty.
7.0	**Invalid Badge and Correct PIN Test (See note 5)**	
7.1	Present Invalid Badge to the reader, and enter a valid PIN.	An invalid credential alarm is received at the workstation. Transaction logged. Door lock does not release.
7.2	Clear the alarm at the workstation.	The active alarm queue is empty.
8.0	**Egress Test**	
8.1	From the secure side of the door, use the push bar to egress.	Request to exit is activated. Door lock releases. Door opens. Door indicates as open at the workstation, but does not alarm.
8.2	Close the door.	Door indicates as closed at the workstation.
9.0	**Door Held Open Test**	
9.1	Open the door.	
9.2	Hold door open until the operator notifies of a door held alarm.	Door held alarm received at workstation within specified time.
9.3	Close the door.	Door indicates as closed at the workstation. Alarm is still active.
9.4	Clear the alarm at the workstation.	The active alarm queue is empty.

Figure 3-5. Sample Card Reader Door Configuration.



Title: Vehicle Gate

Objective: Verify device is installed using acceptable standards and practices, communicates properly with the Access Control System (ACS), and provides proper protection of assets and meets or exceeds the contract performance specification.

Applicability: Gates and site access. Access control systems.

Notes:

1. These procedures are based on a system consisting of a sliding vehicle gate with entry reader, safety sensor loop, and exit sensor loop.
2. Assumes a single credential required for entry (i.e. card only).
3. Perform valid and invalid credential tests for entry.
4. The cards to be prepared prior to testing and used for these tests are as follows:
   Card 1: Authorized to access all areas.
   Card 2: Time zone restricted card. Valid for only normal duty hours.
   Card 3: Time zone restricted card. Valid for only non-duty hours.
   Card 4: Enrolled user with expired access.
   Card 5: Un-programmed card.
   Card 6: Card with insufficient access permissions.
5. For Valid Credential Tests (Step 1.0), use cards 1 and 2.
6. For Invalid Credential Tests (Step 2.0), use cards 3, 4, 5, and 6.
7. Real-time voice communications between the workstation operator and the field technician is required.
8. Line Supervision, Power Fail, and Tamper Tests need to be performed in addition to these procedures.
9. Perform these tests with the associated zone in the SECURE state.

Steps	Actions	Expected Results
1.0	**Valid Credential Access Test**	
1.1	Approach gate with vehicle from the unsecure side.	Gate does not open. No alarm received.
1.2	Present a valid credential to the reader.	Transaction logged at workstation. Gate opens while sounding local area buzzer.
1.3	Drive through the gate.	After appropriate hold time, gate closes while sounding local area buzzer.
2.0	**Invalid Credential Access Test** (see note 3)	
2.1	Present Invalid credential to the reader.	An invalid credential alarm is received at the workstation. Gate does not open.
2.2	Clear the alarm at the workstation.	The active alarm queue is empty.
3.0	**Safety Loop Test**	
3.1	Present a valid credential to the reader.	Transaction logged at workstation. Gate opens while sounding local area buzzer.
3.2	Place a metal plate on the safety loop.	After appropriate hold time, gate does not close. Gate sounds local area buzzer. Blocked gate alarm received at workstation.
3.3	Remove the metal plate and clear the alarm at the workstation.	Gate closes while sounding local area buzzer. The active alarm queue is empty.

Steps	Actions	Expected Results
3.4	Present a valid credential to the reader.	Transaction logged at workstation. Gate opens while sounding local area buzzer.
3.5	Drive into the gate path and stop.	After appropriate hold time, gate does not close. Gate sounds local area buzzer. Blocked gate alarm received at workstation.
3.6	Move vehicle away from gate.	Gate does closes while sounding local area buzzer. Blocked gate alarm still active at workstation.
3.7	Clear the alarm at the workstation.	The active alarm queue is empty.
4.0	**Vehicle Block Test**	
4.1	Present a valid credential to the reader.	Transaction logged. Gate opens.
4.2	Stand Near the gate path, being careful not to block the path of the gate.	After appropriate hold time, gate does not close. Gate sounds local area buzzer. Blocked gate alarm received at workstation.
4.3	Walk away from gate.	Gate does closes while sounding local area buzzer. Blocked gate alarm still active at workstation.
4.4	Clear the alarm at the workstation.	The active alarm queue is empty.
5.0	**Exit Test**	
5.1	Drive vehicle to gate from the inside.	Gate opens while sounding local area buzzer. No alarm received.
5.2	Drive through the gate.	After appropriate hold time, gate closes while sounding local area buzzer.