Explanation of UL 827 Requirements

By paragraph number

Section 11 – Power Supply

11.5.1 Secondary Power

- Prior to 4/11/2019, all stations had 3 secondary power options – batteries only, generator plus 4 hours of battery/UPS, or 2 or more generators
- The new requirements prescribe minimum specific configurations, based on a station's MEW

  calculation

Table 11.1
Secondary power configurations

MEW	# of units	# Auto start	#Assuming load	# Manual start	Capacity of batteries	1st fault	2nd fault
≤999	0	0	0	0	24 hr	Battery supply	None
≤49,999	1	1	1	0	4 hr[b]	Generator	4 hr battery
≥50,000	2	2	1	1	15 min[b]	Generator	Generator
≥50,000	2[a]	2	1	0	15 min[b]	Generator	Generator
≥100,000	2[a]	2	1	0	15 min[b]	Generator	Generator

[a] This is an N+ resilient-configuration in which two or more generators start at the same time with at least one assuming the load.

[b] The battery supply is intended to provide continuity of power during the transition between primary power and the generator(s) assuming the load, or between the first generator and the second generator(s) in the event of a failure of the first generator (See 11.6).

- A station must use the minimum configuration specified for its calculated MEW, ***or may elect*** to use a method for any MEW larger than its calculated value.
- **Please be ready to demonstrate compliance by preparing secondary power arrangement schematics, equipment list, and a narrative of operations if one is necessary. UL staff will also review the physical installation.**

11.7.1 – Storage Battery Type

- Reworded for clarity batteries - Storage batteries need to be designed for stationary commercial or industrial applications in which they are subject to deep discharge or deep cycling.

11.7.4 – Battery Marking

- Storage batteries must be marked with the date they were manufactured

and the date of replacement, based on the manufacturer's data for their life expectancy.

- The marking needs to be on the batteries, displayed on the battery cabinet, or on the control panel of a UPS to which the batteries are connected.
- Going forward, batteries shall be replaced sooner than the marked date if tests indicate that they should be replaced.
- **Please be prepared to demonstrate compliance by showing UL staff how your batteries are marked.**

11.7.5 (NEW) – Battery Installation & Maintenance

- Batteries need to be installed and maintained in accordance with the manufacturer's instructions for safety and continued operation.
- Local codes that apply to installation and safety concerns related to storage batteries must be followed where there is conflict between manufacturer's instructions and direction from the local authority having jurisdiction.

11.8.1 - Overcurrent protection for external batteries

- For batteries that are external to the equipment they power, mechanical enclosure and wiring protection is a new alternative to overcurrent protection in power leads.
- Batteries can be housed in a vented enclosure with wiring between this enclosure and the equipment housed in conduit or EMT (11.8.1 b).

11.9 – Battery Charging Method

- Reworded for clarity

11.10A - Trickle- or float-charged batteries

- Edited, reorganized for clarity and replaces Section 11.10
- 11.10A.7 – When batteries are connected to an Uninterruptible Power Supply (UPS) that can conduct a self-test, that self-test feature may be used as an alternative to the tests described in 11.10A.5 and 11.10A.6.

11.12 A – Stationary, engine-driven generators

- Edited, reorganized for clarity and replaces Section 11.12
- 11.12A.4 – Engine-driven generator maintenance – adds trained central station personnel as an alternative to contracted service provider.

11.13 Security of secondary power supplies

- 11.13.1, 11.13.5, 11.13.6 – edited for clarity, supervised contacts or the equivalent need to be monitored in the operating room.
- 11.13.9
    - Unifies requirements for all fuel shut-off valves, allowing deletion of 11.13.10.

- Reduces the distance between station and shut-off valves that require supervision from 150 ft to 100 ft.
- Adds alternatives for valve supervision including intrusion detection equipment, video surveillance equipment, or construction of a locked enclosure that's acceptable to local authorities.

11.14 A - Uninterruptible power supply units

- Edited, reorganized for clarity and replaces Section 11.14
- 11.14A.7 – NEW – Requires that batteries connected to a UPS meet the UPS manufacturer's specifications.
- **Please be prepared to demonstrate compliance with documentation that shows your batteries meet UPS battery specifications.**

11.15A – Alternate secondary power sources

- Edits material covering uninterruptible battery supplies for clarity and adds options such as diesel rotary uninterruptible power supplies (DRUPS) or renewable energy sources such as photovoltaic wind.

Section 12 – Communication Infrastructure

This section had its last major modification/updating in 1999. Since then many new protection techniques have come about and a lot of history demonstrating what can be expected to occur to communications cabling enter the central station. There have also been major shifts in what is permitted by utilities, who very often provide the cabling for our communication links. With today's modern surveillance techniques, it is often not necessary to provide physical protection.

None of the revisions to Section 12 require action by a Central Station to achieve compliance. UL staff will also review the changes during the annual audit. UL staff will also review the changes during the annual audit.

Revisions fall into 1 of 3 categories:

1) Editorial changes intended to improve clarity
2) Language changes intended to express requirements in a "performance based" manner that focuses on desired outcomes, rather than a "prescriptive based" way that specifies a limited set of exact techniques
3) Addition of surveillance or other techniques as alternatives to physical securement or electrical supervision

With respect to 2:

- Examples of revisions that state requirements in a performance-based manner include:
    - Replacing the phrase “protected against fire, mechanical damage, and attack” with “protect against damage that could impair or prohibit the delivery of central station services”
    - Revised Sections include 12.1.3, 12.1.4, 12.2.1

With respect to 3:

- Language calling for mechanical securement/protection, electrical supervision, or similar has been supplemented with a list of access restriction options that includes both the previously specified methods plus:
    - Layers of complementary security controls which restrict access to the cables and which are monitored in the operating room by video cameras or other electronic security means; or
    - Other means that provide notice to the operators when access to the area housing the cables is made.

  Revised Sections include – 12.2.2, 12.3.1, 12.4.2, 12.5.4, 12.5.5, 12.5.6.1, 12.5.6.2

Section 17 – Automation Systems, Sec 13 - Subsidiary Stations, Sec 14 -Remote Signal Management Center

Revisions to Sec 17, Sec13, Sec 14 and accompanying Sec 5 definitions were adopted with the following rationale from the 12/14/2018 STP Ballot Bulletin):

Industries such as ours are moving into an era where much of what we do is being completely done through the use of direct communications (electronic), rather than person to person. Virtually every service person obtains, is directed, executes and finishes his/her daily assignments without human interaction. The result is a much more efficient and well-documented record of an employee’s daily assignments. Also, database entry is being done remotely by such entities as a remote field office, a dealer, subscribers, and the like. In addition, there is a need to manage the data each level and location of the user is permitted to access and/or change. Along with this “direct communication” (electronic) is the need to ensure the “electronic communications” path that is exposed to “outsiders” (who could interfere, modify, and/or be privy to its content) is protected. This section addresses both issues - data-integrity and secure communications.

New or revised definitions in Sec 5, Glossary include:

5.2.8.1 CERTIFICATE AUTHORITY (CA)
5.2.21 ENCRYPTION, ADVANCED
5.2.28.1 INDEPENDENT DEALER
5.2.29.1 LOCAL AREA NETWORK (LAN)
5.2.47.1 REMOTE DATA ENTRY FACILITY
5.2.66 WIDE AREA NETWORK (WAN)

These terms are used in new or revised requirements elsewhere in the Standard.

Revisions to requirements include:

13.1 – Subsidiary Station connection to central station or residential monitoring station

- Adds requirement that channels meet the applicable requirements of 17.12
- **Central Station companies operating subsidiary stations should be prepared to demonstrate compliance with this requirement by treating the subsidiary station connections as WAN connections in their compliance with requirements in Sec 17.12**

14.2 A – Remote Signal Management Center connection to central station or residential monitoring station

- Clarifies existing requirements and adds requirement that channels meet the applicable requirements of 17.12
- **Central Station companies operating remote signal management centers should be prepared to demonstrate compliance with this requirement by treating the signal management center connections as WAN connections in their compliance with requirements in Sec 17.12**

17.6 Minimum MEW factor requirements

- 17.6.1.2 j) – for all MEW levels, adds items required to be included on dated diagram or printed description of the current configuration of the alarm monitoring automation system
  - 7) All communications channels that enter into the operating room; and
  - 8) All WAN communications channels that penetrate the Central-station company facilities, that connect into the LAN
- **Please be prepared to demonstrate compliance with a network diagram that documents communications channels that enter the operating room and all WAN channels connected to the station's LAN. Though not specifically required by this paragraph, auditing for compliance with Table 17.4 will be greatly expedited if the network diagram also labels communication channels with the applicable Table 17.4 Type designation.**

17.6.3 MEW Factor 10,000 to 99,999

- 17.3.6.3 c) – When a central station locates required IT components in a remote location connecting channels are required to meet the applicable requirements of 17.12
- **Central Station companies that locate required IT components in a remote location should be prepared to demonstrate compliance with this requirement by treating the remote connections as WAN connections in their compliance with requirements in Sec 17.12.**

17.12 Connections to the automation system

- 17.12.2 – Adds requirement that equipment at the remote end of a connection meet the requirements of Sec 17

Table 17.4
Logical security measures for communications with the automation system

Type	Location	Equipment	Security measures[a]
A	Within the operating room	Terminals and servers	Program access control
		Software-based receivers	WAN Security
B	Within the central-station company, but outside of the operating room	Terminals, servers, and printers	Program access controls
C	Remote to the central-station location, not operated by the central-station company, (e,g, independent dealer and the like)	Terminals, servers, and printers	WAN Security and program access control
D	Redundant site (central-station)	Workstations, servers, and printers	WAN Security at both sites and program access control
E	Software vendor support connections and applications	Terminals	WAN Security and program access control
F	Central-station company-owned locations	Terminals	WAN Security and program access control
G	Access to Corporate Network	LAN/ WAN	Assignment of Domain Level Access privileges

[a] See Table 17.5 for program access control requirements

- Table 17.4 – Referenced in 17.12.2 =- revised to reflect changes in requirements for “Logical security measures for communications with the automation system”
  - Note that Type G communications (between automation system and corporate network) are required to employ “Assignment of Domain Level Access privileges” as a security measure, implying network segregation techniques in today’s technology.
  - Also see Table 17.6, item iii – Account and Password Management and Appendix C, item 5, which requires an answer to the question “Do you have policies and standards covering electronic authentication,

authorization, and access control of personnel and resources to your information systems, applications and data?"

- 17.12.5.1 – Where WAN Security measures are called for, requires that, at all times, communication paths employ advanced encryption and measures specified in Sec 17.15.
    - Also requires that systems providing security measures be maintained with the latest updates supplied by the manufacturer.
- 17.12.6 a) 2) – Definition of LAN simplified
    - If any part of the local area network that is not physically secured, managed and under direct control/supervision of the central-station company, the WAN Security measures, as outlined below, shall be applied.
- 17.12.6 a) 3) – Specification of WAN security measures simplified
    - All communications shall employ the use of advanced encryption and other measures as documented (See Appendix D), all of which shall be active at all times. These systems shall be maintained with the latest updates supplied by the manufacturer.
    - Related with respect to latest updates - 17.15.3 – Requires a central station to stay aware of current/evolving cybersecurity issues and threats.

- 17.12.6 a1) – For web app/browser based WAN connections, in combination with glossary definition 5.2.21, definition of evidence of compliance with advanced encryption requirement is specified as digital security certificate issued by a authority (CA) that is accepted and trusted by the browser(s) and the browser client.

- 17.12.6 a2) – For Layer2/IPSec (or similar) based WAN connections, in combination with glossary definition 5.2.21, definition of evidence of compliance with advanced encryption requirement is specified as use of an encryption that is listed in the most recent edition of NIST 800-131 as 'approved and/or acceptable'.

- Using the network diagram described in 17.6.1.2, please be prepared to demonstrate to the UL auditor how compliance with Table 17.4 is achieved for each connection to the automation system.

- 17.12.6 b) revises requirements for temporary connections to add clarity.
  8) adds requirement to employ access control requirements specified in Table 17.5.

17.12A (NEW) Facilities remote from the central-station – enumerates requirements

for central station connections to Independent dealers, Remote data entry facilities, and Service centers, Technicians, and Subscribers

- 17.12A.1.1 - Requires the connection at the central-station be protected and restricted per Tables 17.4 and 17.5.
- 17.12A.1.2 – Prohibits signal handling outside a UL827 complaint operating room
    - Also enumerated in Table 17.5 under Function "Signal requiring operator action"
- 17.12A.1.3 – Requires that personnel of the central-station create and assign the login of remote facility personnel. "Self-service" account creation is not permitted.
    - Also enumerated in Table 17.5 under "Administer, maintain, configure, automation user access".
- 17.12A.1.4 – Requires that connected facilities remote from the central-station be provided with physical access security measures.
    - Those measures need to be documented per 17.5.5 and Table 17.6, item 5. Also see Appendix C, Item 5
- 17.12A.2 Independent dealer – requires that dealer staff be trained and allows a central station to authorize dealer staff to modify data per Table 17.5
    - Please be prepared to share with UL auditor the methods, procedures, practices used to assure that dealer data personnel are trained for automation data entry.
    - Please be prepared to share records of dealer staff training for UL audit
- 17.12A.3 Remote data entry facility – Requires a contractual 30 day notice of intent to cancel/amend agreement, requires that dealer staff be trained and allows a central station to authorize dealer staff to modify data per Table 17.5.
    - Please be prepared to share with the UL auditor
        - The portion of the contract which calls for 30-day intent for each remote data entry facility/company you use
        - The methods, procedures, practices used to assure that remote data entry personnel are trained for automation data entry
        - Records of remote data entry staff training
- 17.12A.4 Service center – Defines a service center and type of staff allowed to modify data per Table 17.5
- Table 17.5 – enumerates access and data edit rights for UL827 compliant operating room staff and for the staff at remote location

Table 17.5
Access and remote functions

Function	Compliant UL 827 c.s. operating room	Service center	Remote data entry center	Independent dealer	Technicians	Subscribers
Security measures	Table 17.4[a]	Table 17.4[a]	Table 17.4[a]	Table 17.4[a]	Table 17.4[a]	Table 17.4[a]
Minimum User ID and Password "Log On" credentials required	Yes	Yes	Yes	Yes	Yes	Yes
Create and/or commission new accounts	Yes	Yes	Yes	Yes	No	No
Administer, maintain, configure, automation user access	Yes	Yes	Yes/No[c]	No	No	No
Administer, configure, or maintain automation data tables	Yes	Yes	Yes/No[c]	No	No	No
Update customer account records	Yes	Yes	Yes	Yes	No	Yes
Permanent schedule changes	Yes	Yes	Yes	Yes	No	Yes
Temporary schedule changes	Yes	Yes	Yes	Yes	No	Yes
Call list updates	Yes	Yes	Yes	Yes	No	Yes
View event history	Yes	Yes	Yes	Yes	Yes	Yes
Signal requiring operator action	Yes	No	No	No	No	No
Initial placed "IN" to Service	Yes	Yes	Yes	No	No	No
Accounts "OUT" of Service	Yes	Yes	Yes	Yes	No	No
Accounts On/Off Test	Yes	Yes[b]	Yes[b]	Yes[b]	Yes[b]	No/Yes[d]
Remote arming	Yes	No	No	No	No	No
Remote disarming	Yes	No	No	No	No	No
Download panel	Yes	Yes	Yes	Yes	No	No

[a] Security measures for remote access outside of the central-station LAN / WAN or VPN shall be such that access is limited to the allowed actions in the table, that network security, log on user validation and restricted access privileges are in place. (Refer to 17.4).

[b] For defined duration not to exceed 8 hours

[c] Yes, for central-station company personnel, No when contractor personnel

[d] Under conditions set by the Central-Station

17.15 (NEW) Cybersecurity Measures – additional measure to be implemented by central station companies

- Notes
    - The cyber threat environment and threat mitigation technologies are both in states of rapid change and evolution. In order to allow central stations to react to those changes and quickly take advantage of new developments, language in this section was chosen to express requirements in a "performance based" manner that focuses on desired outcomes, rather than a "prescriptive based" way that specifies a limited set of exact techniques
    - Central Stations are encouraged, but not required by these requirements, to use a holistic approach to risk management, such as that outlined in the NIST Cybersecurity Framework, IEC 27001 Standard for Information Security, or similar to guide selection of specific tools/measures that align with their specific risk profile and business needs
    - In the judgement of the Standards Technical Panel for UL827, the following measures represent a minimum set of mitigations against cybersecurity threats common to all companies providing central station monitoring services
- 17.15.2 – Requires an ongoing effort to detect unwanted activity in an

automation system network, using tools that report & document all unwanted events

  - This replaces previous language that prescribed use of a firewall and network intrusion detection system and allows central stations to implement new technologies that may not be known by the same names
  - Please be prepared to share documentation of the tools used at your central station and have reports generated by the tools available for audit.

- 17.15.3 – Requires a central station to stay aware of current/evolving cybersecurity issues and threats
  - At a minimum, central stations can demonstrate compliance with policy and practice that applies security related patches/upgrades to its IT operating systems, automation systems, and supporting network devices & tools.
  - Please be prepared to share documentation of the tools used at your central station and actions taken as a result of learning of new issues.
- 17.15.4 – Requires that precautions be taken to isolate backup data from cybersecurity threats
  - At a minimum, central stations can demonstrate compliance with policy and practice that mitigates the risk of ransomware attacks corrupting last known good backups.
  - Please be prepared to share documentation of the tools used at your central station.
- 17.15.5 –By reference to Table 17.6, requires that 18 individual measures, covering 8 specific topics, be put in place by central station companies
  - The language of subject area questions in Appendix C is intended to clarify the intent of requirements in Table 17.6
  - Because the threat profile, business risk tolerance, asset availability, company culture, and other characteristics are unique to each central station, these requirements do not prescribe specifics associated with each cybersecurity measure. Rather, compliance is judge on the basis of whether or not a station company has done its own due diligence and has implemented policies, plans, actions or other measures appropriate that are for its own situation.
  - Please be prepared to share the policies, documentation of processes and procedures, standards, plans, training records or other material address in Table 17.6 and account for them in a form such as/similar to that in UL827, Appendix C.
  - UL staff will examine documents that satisfy the requirements of Table 17.6 for evidence that they have been approved/endorsed by a member of the Central Station's management team.

Table 17.6
Correlation table for Appendix C

Topic	Individual item	(Yes/No/NA)[a]
i, Personnel Security	1, Background security	(Y or N)
	2. Terminated personnel security measures	(Y or N)
ii. Physical Security	3. Access security	(Y or N)
	4, Workstations secured	(Y or N)
iii. Account and Password Management	5. Access into the automation system(s)	(Y or N)
iv. Confidentiality of Sensitive Data	6. Retention policy(s)	(Y or N)
	7, Archival policy(s)	(Y or N)
	8. Disposing of materials policy(s)	(Y or N)
v. Disaster Recovery	9. Business continuity plan(s) (See 19.2)	(Y or N)
	10, Backup/archival policy(s)	(Y or N)
vi. Security Awareness and Education	11. Staff awareness policy(s):	(Y/N/NA)
	12. Staff alertness to possible breaches, policy(s):	(Y/N/NA)
	13. Password security awareness policy (s)	(Y or N)
vii. Cybersecurity (See Appendix E for communications examples)	14. Exiting communication channels identified (See 17.6.1.2(j)	(Y or N)
	15, Vulnerable channels identified (Y or N):	(Y or N)
	16. Actions to mitigate taken and recorded:	(Y/N/NA)
	17. Actions taken to secured data and recorded:	(Y/N/NA)
viii, Actions Taken on Vulnerable Channels	Based upon the analysis in the above section vii Cybersecurity, and those channels identified as vulnerable, proceed to document any observations and the corrective measures take to protect against cyber-attacks.	
The form shall be updated as elements change, but no less than twice annually		
Numbering corresponds to numbering on the form		

[a] The items that are marked with a "Y or N" shall be addressed and documentation kept thereof. Unmarked items are those that are dependent upon the configuration of the subject central-station.