UL 827 Permanent Work From Home Review

VIRTUAL OPERATOR WORKSPACE

Javier Olarte
UL Solutions

Virtual Operator Workspace sections

- 37 General
- 38 Operation Within the Central-Station
- 39.1 Bandwidth and connectivity
- 39.2 Remote operator workstation
- 39.3 Workplace environment
- 39.4 Central-station compliance verification

37 General

- 37.1 A central-station company may employ remotely located operators to process signals from any system except those that comply with UL 2050, ULC S301 or ULC S561.
- When the MEW factor requires there be two or more central-stations, as referenced in 17.6.4, MEW Factor 100,000 or greater, the operators working remotely in support of the redundant site, shall also be diverse as referenced in 17.6.4.2.

38 Operation Within the Central-Station

- 38.1 The central-station company shall not be unstaffed at any time.

- 38.2 Staffing shall be by central-station company employees trained to perform tasks in the manner and timeframes required by this Standard.

39.1 Bandwidth and connectivity

- 39.1.1 The data and voice communication technology connections required for remote operators to perform their job functions shall be made to the central-station company network through a secure, remote access technology (e.g. virtual private network (VPN), virtual desktop infrastructure (VDI) and remote desktop protocol (RPD) that complies with 17.11, Connections to the automation system, for the remote workstation to the network at the monitoring station or automation system host.
- 39.1.2 The remote access technology specified in 39.1.1 shall be deployed in a manner such that the remote employee is required to use some form of two multi-factor authentication (MFA) in order to gain access to the workstation, central-station company network and or automation systems

39.1 Bandwidth and connectivity

- 39.1.3 Communication between a remote operator workstation and the central-station company shall comply with (a) and (b); or (c) and (d) as follows:

a) There shall be primary and backup communication connections between the remote operator workstation and the central-station company complying with 12.1.6.

b) The workstation, router, and networking equipment necessary to support communication with the central-station company shall be powered by an uninterruptible power supply that has battery backup for the amount of time needed to transfer active alarm(s) to another operator.

c) There shall be sufficient operators on-duty and logged into the automation system, so that loss of communication between a remote operator workstation and the central-station company will not result in the loss of any signals or failure to process signals in the manner and timeframes required by this Standard.

d) System and workstation monitoring shall be in place to ensure 99.95 % connectivity between workstations and the monitoring center during the time an operator is handling alarms. Connectivity is to be measured as all operator alarm handling time during a rolling 30-day period. Central-station company shall maintain and retain data to substantiate that this connectivity requirement is met.

39.2 Remote operator workstation

- 39.2.1 Remote operator workstation equipment shall comply with the requirements of this Standard applicable to the type of equipment and shall be configured and controlled by the central-station company as follows:

  a) The workstation equipment shall be configured and maintained by enrollment in the central-station company processes; and

  1) Antivirus/antimalware shall be installed, enabled and functioning;

  2) Windows or other operating system security patches and updates shall be applied; and

  3) The central-station company shall have policies and controls in place to manage access to USB devices and the tools to monitor access and use of any connected USB or storage devices.

  b) If the automation system operation stores data on the remote operator workstation, then the workstation shall be protected with whole disk encryption with provision for a system administrator password that meets Section 7.12.6 Part (B), Items (1-4) of NIST 800-63-3.

- 39.2.2 The remote operator workstation shall employ a means to send a duress signal to the central-station company using the capability referenced in the Sign-on security levels section in UL 1981.

UL 1981 – Central-Station Automation Systems

- 5.37A OPERATOR DURESS SIGNAL – An automation system key(s) stroke or other function, that a remote operator performs, to alert the Central Station they are in duress.

- 6.3.9 A operator duress signal function shall be available in the automation software. The intent is to allow a remote operator to signal to the Central station that they are in duress. Upon receiving the duress signal the automation shall:

  a) Restrict the workstation's access to subscriber data through the automation system or other means,

  b) Notify a designated recipient, that the operator has reported he/she is under duress;

  c) Log the event; and

  d) Re-establishing full communications to the automation system shall require action by the managing central-station, after the duress incident has been resolved.

39.3 Workplace environment

- 39.3.1 Remote operators shall maintain a work area that complies with the following:

  a) Work area is located in a closed room not occupied by any other individual while the operator is on duty;

  b) The operator's workstation screen shall not be visible to another person located either inside or outside the premises; and

  c) Operators shall use headsets to provide audio obscuration of incoming voice signal.

- 39.3.2 To facilitate compliance verification, the central-station company shall arrange for the following requirements to be met:

  a) Video recording devices shall be deployed which provide a field of view that includes the operator and surrounding work area; and

  b) The central-station company shall have the ability to capture the operator's screen content.

39.3 Workplace environment

- 39.3.3 Prior to a remotely located operator's first duty shift, central-station company shall verify and document that the remote location workspace complies with 39.3.1. Documentation shall include:

  a) Identification of the verifier and the remote workstation and workspace;

  b) Date of verification;

  c) Means by which compliance was determined (physical inspection, virtual tour, other as appropriate);

  d) Central-station company records shall be retained for a minimum of twelve months (refer to 19.7.1); and

  e) Verifications of workstation workspace should be performed upon initial deployment and periodically thereafter to ensure that the workspace has not changed.

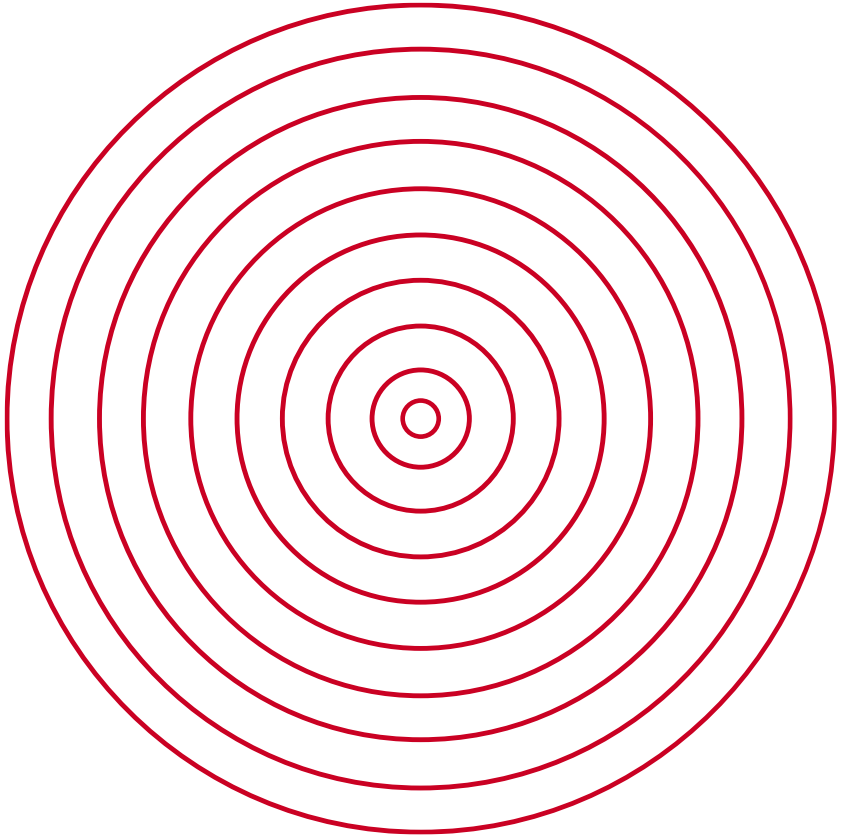
39.3 Workplace environment

- 39.3.4 The central-station company shall employ a means by which the managing central-station company can communicate with and supervise (audio, visual or otherwise) the remote employees as required to fulfill monitoring responsibilities.
- 39.3.5 The central-station company shall document the security architecture of the implemented remote operator station.
- 39.3.6 The security architecture documentation shall be made part of the central-station company business continuity plans described in Table 17.4 Item (v), 18.2.2.
- 39.3.7 The central-station company shall provide remote operators with training on current cyber and information security issues impacting their environment and the central-station company security policies to mitigate security related risks

39.4 Central-station compliance verification

- 39.4.1 The central-station company shall re-verify compliance with workplace environment requirements in 39.3.1 using information from the sources described in 39.3.2 and any others deemed appropriate for the specific arrangement by the central-station company.
- 39.4.2 The central-station company shall conduct a complete review of the physical workspaces at least once per year. Documentation shall include:
  - a) Identification of the verifier and the remote location;
  - b) Date of verification;
  - c) Means by which compliance was determined (physical inspection, virtual tour, other as appropriate); and
  - d) Any items of non-compliance and dated description of corrective action taken.

Questions?



Javier Olarte

UL.com/Solutions

Thank you

UL.com/Solutions

Safety. Science. Transformation.™