TCVN **TIÊU CHUẨN QUỐC GIA**

TCVN …….. :2025

Xuất bản lần 1

DỰ THẢO

PHÒNG CHÁY CHỮA CHÁY – HỆ THỐNG TRUYỀN TIN BÁO SỰ CỐ

Fire protection – Alarm transmission system

HÀ NỘI - 2025

Mục lục

Lời nói đầu **4**

1 Phạm vi áp dụng **5**

2 Tài liệu viện dẫn **5**

3 Thuật ngữ, định nghĩa và ký hiệu **6**

4 Quy định chung **15**

5 Yêu cầu đối với hệ thống truyền tin báo sự cố **15**

5.1 Yêu cầu chung 16

5.2 Yêu cầu liên kết truyền dẫn 16

5.3 Yêu cầu hiệu suất 18

5.4 Bảo đảm an toàn cho các thông báo 19

5.5 Xác nhận truyền báo động 20

5.6 Cảnh báo do ATS tạo ra 20

5.7 Tính khả dụng 20

5.8 Bảo mật 21

5.9 Giải pháp ATS lưu trữ 22

5.10 Tài liệu hướng dẫn 23

6 Yêu cầu đối với thiết bị thu phát tại cơ sở giám sát (SPT) **23**

6.1 Yêu cầu chức năng của SPT 23

6.2 Yêu cầu thiết kế 27

6.3 Những yêu cầu thiết kế bổ sung đối với SPT điều khiển bằng phần mềm 31

6.4 Yêu cầu về ghi nhãn 33

7 Yêu cầu đối với thiết bị thu phát tại trung tâm tiếp nhận (RCT) **33**

7.1 Yêu cầu chung 33

7.2 Yêu cầu về cấp quyền truy cập logic 34

7.3 Tải lên và tải xuống phần mềm 34

7.4 Lưu trữ các thông số và dữ liệu 35

7.5 Giám sát và thông báo lỗi của ATP và ATS 35

7.6 Giao diện tới AMS 35

7.7 Tín hiệu lỗi 35

7.8 Ghi lại sự kiện 35

7.9 Chế độ vận hành (lưu và chuyển tiếp hoặc truyền thẳng) 36

7.10 Từ chối dịch vụ 37

7.11 Bảo mật thông tin 37

7.12 Bảo mật chống giả mạo 37
7.13 RCT dự phòng 37
7.14 Tài liệu 38
7.15 Ghi nhãn 38
8 Yêu cầu đối với truy cập từ xa 38
8.1 Yêu cầu chung 38
8.2 Yêu cầu đối với bảo mật thông tin 39
8.3 Yêu cầu về hiệu suất 41
8.4 Yêu cầu về chức năng 41
8.5 Yêu cầu vận hành 42
9 Kiểm tra, thử nghiệm 42
9.1 Kiểm tra hiệu suất ATS 42
9.2 Kiểm tra, thử nghiệm SPT 46
9.3 Kiểm tra, thử nghiệm RCT 49
Phụ lục A (tham khảo) Cấu trúc logic ATS **52**
Phụ lục B (tham khảo) Tính khả dụng **54**
Phụ lục C (quy định) Mức truy cập **56**
Phụ lục D (quy định) Chương trình kiểm tra SPT **57**
Phụ lục E (quy định) Chương trình kiểm tra RCT **78**
Phụ lục F (quy định) Giao diện FDAD và SPT **88**
Thư mục tài liệu tham khảo 89

Lời nói đầu

TCVN .....:2025 do Cục Cảnh sát phòng cháy, chữa cháy và cứu nạn, cứu hộ biên soạn, Bộ Công an đề nghị, Ủy ban Tiêu chuẩn Đo lường Chất lượng Quốc gia thẩm định, Bộ Khoa học và Công nghệ công bố.

Phòng cháy chữa cháy – Hệ thống truyền tin báo sự cố

Fire protection – Alarm transmission system

1 Phạm vi áp dụng

1.1 Tiêu chuẩn này quy định yêu cầu kỹ thuật, phương pháp thử nhằm đánh giá hiệu suất, độ tin cậy và bảo mật của hệ thống, các thiết bị thuộc hệ thống truyền tin báo sự cố và các yêu cầu cơ bản đối với cơ sở hạ tầng truy cập từ xa phục vụ người sử dụng để có thể tiếp nhận thông tin báo cháy qua hệ thống truyền tin báo sự cố.

1.2 Hệ thống truyền tin báo sự cố và các thiết bị của hệ thống truyền tin báo sự cố ngoài tuân thủ các quy định tại tiêu chuẩn này còn phải đáp ứng các quy định khác của pháp luật hiện hành có liên quan.

2 Tài liệu viện dẫn

Các tài liệu viện dẫn dưới đây rất cần thiết khi áp dụng tiêu chuẩn này. Đối với các tài liệu có ghi năm công bố thì áp dụng phiên bản đã nêu. Đối với các tài liệu không ghi năm công bố thì áp dụng phiên bản mới nhất (bao gồm cả sửa đổi).

TCVN 4255 (IEC 60529) Cấp bảo vệ bằng vỏ ngoài (mã IP);

TCVN 7568-4 (ISO 7240-4) Hệ thống báo cháy - Phần 4: Thiết bị cấp nguồn;

TCVN 7921-3-3 (IEC 60721-3-3) Phân loại điều kiện môi trường - Phần 3-3: Phân loại theo nhóm các tham số môi trường và độ khắc nghiệt - sử dụng tĩnh tại ở vị trí được bảo vệ khỏi thời tiết;

TCVN 7699-1 (IEC 60068-1) Thử nghiệm môi trường - Phần 1: Quy định chung và hướng dẫn;

TCVN 7699-2-1 (IEC 60068-2-1) Thử nghiệm môi trường - Phần 2-1: Các thử nghiệm - Thử nghiệm A: Lạnh;

TCVN 7699-2-6 (IEC 60068-2-6) Thử nghiệm môi trường - Phần 2-6: Các thử nghiệm - Thử nghiệm FC: Rung (hình sin);

TCVN 7699-2-47 (IEC 60068-2-47) Thử nghiệm môi trường - Phần 2-47: Các thử nghiệm - Lắp đặt mẫu để thử nghiệm rung, va chạm và lực động tương tự;

TCVN 7699-2-75 (IEC 60068-2-75) Thử nghiệm môi trường - Phần 2-75: Các thử nghiệm - Thử nghiệm Eh: Thử nghiệm búa;

TCVN 7699-2-78 (IEC 60068-2-78) Thử nghiệm môi trường - Phần 2-78: Các thử nghiệm - Thử nghiệm Cab: Nóng ẩm, không đổi;

TCVN 11367 (ISO/IEC 18033) (tất cả các phần) Công nghệ thông tin - Các kỹ thuật an toàn - Thuật toán mật mã;

TCVN 11816 (ISO/IEC 10118) (tất cả các phần) Công nghệ thông tin - Các kỹ thuật an toàn - Hàm băm.

3 Thuật ngữ, định nghĩa và viết tắt

3.1 Tiêu chuẩn này áp dụng các thuật ngữ và định nghĩa sau:

3.1.1

ATS đường truyền đơn (single path ATS)

ATS (hệ thống truyền tin báo sự cố, xem 3.1.18) có một ATP (đường truyền báo động, xem 3.1.12) để kết nối một hoặc nhiều FDAD (thiết bị báo cháy, xem 3.1.38) của một cơ sở được giám sát với một hoặc nhiều AE (thiết bị thông báo, xem 3.1.39) của một hoặc nhiều ARC (trung tâm tiếp nhận báo động, xem 3.1.36).

3.1.2

ATS đường truyền kép (dual path ATS)

ATS bao gồm một ATP chính và một ATP dự phòng được sử dụng công nghệ đa dạng (xem 3.1.7), có hai giao diện mạng truyền dẫn tại SPT (thiết bị thu phát tại cơ sở được giám sát, xem 3.1.41), để kết nối một hoặc nhiều FDAD của một cơ sở được giám sát với một hoặc nhiều AE của một hoặc nhiều ARC.

3.1.3

ATS nhiều đường truyền (multiple path ATS)

ATS trong đó nhiều hơn một ATP được sử dụng kết hợp để kết nối một hoặc nhiều FDAD của một cơ sở được giám sát với một hoặc nhiều AE của một hoặc nhiều ARC.

3.1.4

Bảo mật tín hiệu (signalling security)

Các phương pháp sử dụng để ngăn chặn hoặc phát hiện các nỗ lực cố ý can thiệp vào quá trình truyền một báo động bằng cách chặn hoặc giả mạo.

3.1.5

Chỉ báo (indication)

Thông tin (bằng âm thanh, hình ảnh hoặc bất kỳ hình thức nào khác) về trạng thái của SPT, RCT (thiết bị thu phát tại trung tâm tiếp nhận, xem 3.1.40) và/hoặc ATS.

3.1.6

Chủng loại ATS (ATS category)

Bộ thông số xác định các yêu cầu về hiệu suất của ATS.

Ghi chú: Chủng loại ATS được xác định bởi các yêu cầu tối thiểu đối với ATS.

3.1.7

Công nghệ đa dạng (diverse technology)

Các công nghệ được sử dụng trong các đường truyền theo cách mà một điểm lỗi đơn lẻ hoặc việc can thiệp vào một điểm duy nhất không thể khiến cả hai đường truyền trong hệ thống có đường dẫn kép bị lỗi đồng thời.

Ghi chú: Ví dụ để tránh hai đường truyền bị gián đoạn cùng lúc, các công nghệ khác nhau sẽ được sử dụng cho hai đường truyền, như một đường truyền sử dụng mạng di động (3G/4G/5G), 1 đường truyền sẽ sử dụng mạng cáp quang hoặc mạng cố định.

3.1.8

Cơ sở được giám sát (supervised premises)

Cơ sở được trang bị FDAD nhằm phát hiện nguy cơ cháy.

3.1.9

Dung lượng hệ thống (system capacity)

Số lượng FDAD tối đa mà ATSN (mạng dịch vụ truyền tin báo động, xem 3.1.25) có thể kết nối được.

3.1.10

Đánh giá ngang hàng (peer review)

Khi được sử dụng để tham chiếu đến các thuật toán mật mã, có nghĩa là có bằng chứng đã công bố rằng cộng đồng mật mã đã xác nhận tính mạnh mẽ của thuật toán chống lại các cuộc tấn công.

3.1.11

Điểm truy cập từ xa (Remote Access Endpoint, RAE)

Chức năng logic quản lý truy cập từ xa vào các chức năng của một hoặc nhiều ATS để tiếp nhận, sử dụng thông tin báo động của một hoặc nhiều FDAD.

Ghi chú: Trong tài liệu này, RAE phải được hiểu là các chức năng chứ không phải thiết bị vật lý.

3.1.12

Đường truyền báo động (Alarm transmision path, ATP)

Định tuyến một thông báo báo động di chuyển giữa một FDAD riêng lẻ và AE liên quan.

Ghi chú: ATP bắt đầu tại giao diện giữa FDAD và SPT và kết thúc tại giao diện giữa RCT và AE. Đối với mục đích thông báo và giám sát, hướng ngược lại cũng có thể được sử dụng

3.1.13

Giám sát (monitoring)

Quá trình xác minh các kết nối và thiết bị trong hệ thống hoạt động đúng cách.

3.1.14

Hạ tầng truy cập từ xa (Remote Access Infrastructure, RAI)

Hệ thống bao gồm các chức năng logic của RAE, RAS (máy chủ truy cập từ xa, xem 3.1.27) và RAC (khách hàng truy cập từ xa, xem 3.1.20).

3.1.15

Hệ thống bên thứ ba (Third-Party System)

Hệ thống hoặc ứng dụng giao tiếp với FDAD qua ATS mà không được sản xuất bởi RAISP (Nhà cung cấp dịch vụ hạ tầng truy cập từ xa, xem 3.1.30).

3.1.16 .

Hệ thống quản lý ATS (ATS management system)

Một phần của ATS được sử dụng để quản lý thiết bị truyền báo động, giám sát thiết bị truyền báo động và mạng truyền tín hiệu và có thể giúp duy trì hoạt động của ATS.

Ghi chú : Hệ thống quản lý cũng có thể được sử dụng để thu thập dữ liệu về tính khả dụng của ATS.

3.1.17

Hệ thống quản lý báo động (alarm management system, AMS)

Hệ thống tại MARC (trung tâm giám sát và tiếp nhận báo động) có nhiệm vụ lưu trữ, sắp xếp, kiểm soát, quản lý và cho phép truy xuất dữ liệu của khách hàng và được giao tiếp với RCT để tự động phát thông báo đến SPT.

3.1.18

Hệ thống truyền tin báo sự cố (Alarm transmission system, ATS)

Hệ thống gồm các ATE (thiết bị truyền tin báo động, xem 3.1.35) và mạng truyền tin được sử dụng để truyền thông tin liên quan đến trạng thái của một hoặc nhiều FDAD tại cơ sở được giám sát đến một hoặc nhiều AE của một hoặc nhiều ARC.

Ghi chú: Một ATS có thể bao gồm nhiều hơn một đường truyền báo động.

3.1.19

Kết nối (Connection)

Liên kết truyền thông giữa các phần của hệ thống hoặc thiết bị để trao đổi thông tin.

3.1.20

Khách hàng truy cập từ xa (Remote Access Client, RAC)

Chức năng logic được sử dụng để truy cập từ xa vào các chức năng của một hoặc nhiều ATS.

Ghi chú: Trong tài liệu này, Remote Access Client được coi là một chức năng thay vì một thiết bị vật lý.

3.1.21

Kỹ thuật băm (hashing technique)

Kỹ thuật sử dụng phép biến đổi toán học lấy đầu vào và trả về một chuỗi có kích thước cố định, được gọi là giá trị băm.

Ghi chú: Giá trị băm được sử dụng để phát hiện bất kỳ thay đổi nào của đầu vào và do đó xác minh nội dung một cách dễ dàng

3.1.22

Liên kết truyền dẫn (transmission link)

Một phần của mạng truyền dẫn được sử dụng để mang một hoặc nhiều ATP.

Ghi chú 1: ATP có thể được thiết lập bằng cách chuyển đổi các liên kết truyền dẫn theo nhiều cách (song song, nối tiếp và kết hợp các cách đó).

Ghi chú 2: Một liên kết truyền dẫn có thể mang nhiều ATP hoặc các đoạn của ATP.

3.1.23

Mã hóa (encryption)

Mã hóa có hệ thống một luồng bit trước khi truyền, để thông tin chứa trong luồng bit không thể bị giải mã bởi một bên không được phép.

3.1.24

Mạng chuyển mạch gói (packet switched network)

mạng truyền sử dụng chuyển mạch gói.

Ghi chú 1: Các thông báo được chia thành các gói, được định địa chỉ riêng lẻ và định tuyến qua mạng, có thể sử dụng các tuyến khác nhau. Tại nút cuối, các gói được lắp ráp lại để chuyển đổi trở lại thành thông báo gốc.

Ghi chú 2: Ví dụ nổi bật nhất về mạng dữ liệu chuyển mạch gói là Internet, sử dụng bộ giao thức Internet, được Lực lượng chuyên trách về kỹ thuật liên mạng (IETF) chỉ định trong các Yêu cầu bình luận (RFC).

3.1.25

Mạng dịch vụ truyền báo động (alarm transmission service network, ATSN)

Nhóm các ATS cùng chủng loại.

Ghi chú: Một ATSN bao gồm một hoặc nhiều ATS cùng chủng loại, hoạt động dưới sự giám sát của cùng một trung tâm quản lý và giám sát

3.1.26

Mạng truyền dẫn (transmission network)

Mạng giữa hai hoặc nhiều ATE.

Ghi chú: Trường hợp mạng được cung cấp bởi một nhà cung cấp dịch vụ chung (ví dụ: nhà điều hành mạng điện thoại công

cộng), mạng có thể bao gồm các thiết bị truyền dẫn chung không được quy định tại tiêu chuẩn này, ví dụ: thiết bị của nhà điều hành mạng điện thoại công cộng, thiết bị của nhà điều hành điện thoại di động, modem ADSL, modem SDSL, Bộ định tuyến, Bộ chuyển mạch Ethernet, Hub Ethernet, Tường lửa và hệ thống dây mạng.

3.1.27

Máy chủ truy cập từ xa (Remote Access Server, RAS)

Các chức năng logic được sử dụng để quản lý nhiều kết nối từ xa, cho phép người dùng nhận thông tin báo động từ FDAD qua ATS.

3.1.28

Mức truy cập (Access level)

Một trong nhiều trạng thái của thiết bị, hệ thống trong đó:

- các điều khiển có thể được vận hành;

- các thao tác thủ công có thể được thực hiện;

- các chỉ dẫn có thể nhìn thấy và/hoặc;

- thông tin có thể được thu thập.

Ghi chú: Xem phụ lục C

3.1.29

Nhà cung cấp dịch vụ truyền báo động (alarm transmission service provider, ATSP)

Cá nhân hoặc tổ chức chịu trách nhiệm thiết kế, vận hành, quản lý và xác minh hiệu suất của một hoặc nhiều ATSN.

Ghi chú: ATSP có thể ủy quyền một số trách nhiệm thông qua hợp đồng với khách hàng, MARC, nhà điều hành mạng truyền tải, v.v. nhưng vẫn chịu trách nhiệm tổng thể

3.1.30

Nhà cung cấp dịch vụ hạ tầng truy cập từ xa (Remote Access Infrastructure Service Provider, RAISP)

Tổ chức chịu trách nhiệm thiết kế, vận hành và bảo trì RAI.

3.1.31

Nguồn điện chính (prime power source)

Nguồn điện được sử dụng để cấp điện cho thiết bị trong điều kiện hoạt động bình thường.

3.1.32

Nguồn điện dự phòng (alternative power source)

Nguồn điện có khả năng cấp điện cho thiết bị trong thời gian nhất định khi không có nguồn điện chính.

3.1.33

Người dùng từ xa (Remote User)

Người sử dụng RAI qua RAC để truy cập từ xa vào một hoặc nhiều ATS.

Ghi chú: Người dùng từ xa không nhất thiết là người dùng của ATS.

3.1.34

Phiên làm việc (Session)

Trao đổi thông tin tạm thời và tương tác giữa người dùng truy cập từ xa và ATS hoặc giữa các hệ thống bên thứ ba và ATS.

3.1.35

Thiết bị truyền tin báo động (alarm transmission equipment, ATE)

Thuật ngữ chung để mô tả SPT, MCT và RCT.

3.1.36

Trung tâm tiếp nhận báo động (alarm receiving centre, ARC)

Trung tâm liên tục có người trực mà thông tin liên quan đến trạng thái của một hoặc nhiều FDAD được báo cáo.

3.1.37

Trung tâm giám sát ATS (ATS monitoring centre)

Trung tâm mà trạng thái và hiệu suất của một hoặc nhiều ATS được giám sát.

Ghi chú: Trung tâm giám sát ATS có thể là một trung tâm riêng biệt hoặc là một phần của ARC. Trung tâm giám sát ATS cũng có thể là nơi đặt MCT hoặc nơi đặt hệ thống quản lý.

3.1.38

Thiết bị báo cháy (fire detection and alarm device, FDAD)

Thiết bị hoặc hệ thống phát hiện thủ công hoặc tự động sự hiện diện mối nguy hiểm cháy.

Ghi chú: Thiết bị báo cháy có thể là trung tâm báo cháy và/hoặc các thiết bị báo cháy, phát hiện cháy, nút ấn báo cháy….

3.1.39

Thiết bị thông báo (annunciation equipment, AE)

Thiết bị đặt tại ARC nhằm bảo mật và hiển thị trạng thái báo động hoặc trạng thái báo động đã thay đổi của FDAD để phản hồi khi nhận được báo động đến trước khi gửi xác nhận.

Ghi chú: AE không phải là một phần của ATS

3.1.40

Thiết bị thu phát tại trung tâm tiếp nhận (receiving centre transceiver, RCT)

Thiết bị được đặt tại một vị trí an toàn và có chức năng tối thiểu là nhận và gửi thông báo báo động đến

AMS

Ghi chú: RCT có thể bao gồm các chức năng quản lý cho ATS.

3.1.41

Thiết bị thu phát tại cơ sở được giám sát (supervised premises transceiver, SPT)

ATE tại cơ sở được giám sát bao gồm giao diện tới FDAD và giao diện tới một hoặc nhiều mạng truyền dẫn và là một phần của một hoặc nhiều ATP.

3.1.42

Thiết bị thu phát trung tâm giám sát (monitoring centre transceiver, MCT)

ATE trong ATS cho phép giám sát và quản lý thông tin liên quan đến trạng thái của thiết bị và mạng truyền báo động

Ghi chú: Thiết bị phát trung tâm giám sát có thể được đặt tại trung tâm tiếp nhận báo động hoặc tại một trung tâm riêng biệt

3.1.43

Thiết bị mạng tại chỗ (network equipment on site)

Thiết bị là một phần của ATP, nhưng không được coi là ATE.

3.1.44

Thông báo (message)

Chuỗi tín hiệu được truyền bao gồm nhận dạng, dữ liệu chức năng và các phương tiện khác nhau để cung cấp tính toàn vẹn, khả năng miễn nhiễm và khả năng thu sóng phù hợp của riêng nó

3.1.45

Thông báo được bảo mật (secured message)

Thông báo không thể bị mất (ví dụ: trong trường hợp mất điện) và có thể được truy xuất

3.1.46

Trạng thái báo động (alarm condition)

Trạng thái của FDAD, hoặc một phần của FDAD, phát sinh từ phản ứng của FDAD đối với sự hiện diện của mối nguy hiểm cháy.

Ghi chú: Các trạng thái báo động của FDAD trong tiêu chuẩn này có thể gồm:

- Trạng thái báo động cháy, khi một báo động cháy được FDAD hoặc một phần của FDAD chỉ báo:
- Trạng thái cảnh báo-lỗi, khi một lỗi được FDAD hoặc một phần của FDAD chỉ báo
- Trạng thái tín hiệu giám sát, khi một tín hiệu giám sát được FDAD hoặc một phần của FDAD chỉ báo;
- Trạng thái tắt, khi một lệnh tắt các chức năng được FDAD hoặc một phần của FDAD chỉ báo;
- Trạng thái kiểm tra, khi kiểm tra các chức năng được FDAD hoặc một phần của FDAD chỉ báo;

3.1.47

Tính khả dụng (availability, general)

Phần trăm thời gian hệ thống hoặc các bộ phận của hệ thống hoạt dộng đáp ứng yêu cầu của tiêu chuẩn này

3.1.48

Thông báo/tín hiệu lỗi (fault message/signal)

Thông báo hoặc tín hiệu được tạo ra do trạng thái lỗi

3.1.49

Thời gian báo cáo (reporting time)

Khoảng thời gian từ khi lỗi xảy ra trong ATS cho đến khi thông tin lỗi được báo cáo cho RCT, FDAD tại cơ sở được giám sát và MCT (nếu có).

3.1.50

Thời gian truyền (transmission time)

Thời gian từ khi trạng thái thay đổi xảy ra hoặc thông báo báo động được trình bày để truyền tại giao diện SPT tới FDAD cho đến thời điểm trạng thái hoặc thông báo mới được báo cáo tại giao diện RCT tới AMS.

3.1.51

Trạng thái lỗi (fault condition)

Trạng thái của một hệ thống ngăn hệ thống hoặc một phần của hệ thống hoạt động bình thường

3.1.52

Trung tâm giám sát (monitoring centre)

Trung tâm giám sát trạng thái của một hoặc nhiều ATSN.

3.1.53

Trung tâm giám sát và tiếp nhận báo động (monitoring and alarm receiving centre)

Trung tâm có người trực liên tục, nơi thông tin liên quan đến trạng thái của một hoặc nhiều FDAD được báo cáo và ngoài ra, nơi trạng thái của một hoặc nhiều ATS được giám sát

3.1.54

Truy cập cục bộ (local access)

Truy cập từ bên trong cơ sở được bảo vệ khi cần truy cập vật lý trước khi có thể truy cập logic

3.1.55

Truy cập logic (logical access)

Truy cập dữ liệu (ví dụ: cấu hình, trạng thái, phần mềm)

3.1.56

Truy cập từ xa (remote access)

Quyền truy cập vào thiết bị từ bất kỳ vị trí nào nằm ngoài vị trí đặt thiết bị

3.1.57

RCT lưu trữ (hosted RCT)

RCT bao gồm hai phần, trong đó một phần được đặt ở vị trí an toàn (RCT-H) và một phần khác được cài đặt trong ARC (RCT-A).

3.1.58

Xác thực (authentication)

Trao đổi mã để xác định rằng SPT chưa được thay thế bằng thiết bị tương tự không có mã này hoặc xác định rằng thông tin thông báo được truyền đi chưa bị sửa đổi

3.1.59

Vị trí an toàn (secure location)

Vị trí là MARC hoặc vị trí khác tuân thủ yêu cầu về an ninh, an toàn của trung tâm dữ liệu theo quy định.

3.2 Ký hiệu

Tiêu chuẩn này áp dụng các ký hiệu sau đây

Ký hiệu	**Diễn giải**
ADSL	Đường thuê bao kỹ thuật số không đối xứng (Asymmetric Digital Subscriber Line)
AE	Thiết bị thông báo (Annunciation Equipment)
AMS	Hệ thống quản lý báo động (Alarm Management System)
ARC	Trung tâm tiếp nhận báo động (Alarm Receiving Centre)
ATE	Thiết bị truyền báo động (Alarm Transmission Equipment)
ATP	Đường truyền báo động (Alarm Transmission Path)
ATS	Hệ thống truyền tin báo sự cố (Alarm Transmission System)
ATSN	Mạng dịch vụ truyền báo động (Alarm Transmission Service Network)
ATSP	Nhà cung cấp dịch vụ truyền báo động (Alarm Transmission Service Provider)
DTMF	Tần số đa âm kép (Dual Tone Multi Frequency)
DSL	Đường thuê bao kỹ thuật số (Digital Subscriber Line)
FDAD	Thiết bị báo cháy (Fire Detection and Alarm Device)
GSM	Hệ thống di động toàn cầu (Global System Mobile)

Ký hiệu	Diễn giải
GPRS	Dịch vụ vô tuyến gói chung (General Packet Radio Services)
I_{rcT}	Giao diện của AMS tới RCT (Interface of the AMS to the RCT)
ISO	Tổ chức tiêu chuẩn hóa quốc tế (International Standardisation Organisation)
ISDN	Mạng kỹ thuật số dịch vụ tích hợp (Integrated Service Digital Network)
MARC	Trung tâm giám sát và tiếp nhận báo động (Monitoring and Alarm Receiving Center)
MCT	Thiết bị thu phát trung tâm giám sát (Monitoring Centre Transceiver)
PSN	Mạng chuyển mạch gói (Packet Switched Network)
PSTN	Mạng điện thoại công cộng (Public Switched Telephone Network)
RAC	Khách hàng truy cập từ xa (Remote Access Client)
RAE	Điểm truy cập từ xa (Remote Access Endpoint)
RAI	Hạ tầng truy cập từ xa (Remote Access Infrastructure)
RAS	Máy chủ truy cập từ xa (Remote Access Server)
RAISP	Nhà cung cấp dịch vụ hạ tầng truy cập từ xa (Remote Access Infrastructure Service Provider)
RCT	Thiết bị thu phát trung tâm trung tâm tiếp nhận (Receiving Centre Transceiver)
RCT-A	Một phần của RCT lưu trữ được cài đặt trong ARC, đối tác của RCT-H (Receiving Centre Transceiver)
RCT-H	Một phần lưu trữ của RCT được sử dụng trong giải pháp ATS lưu trữ (Hosted part of the RCT used in a hosted ATS solution)
SPT	Thiết bị thu phát tại cơ sở được giám sát (Supervised Premises Transceiver)
SDSL	Đường thuê bao kỹ thuật số đối xứng (Symmetric Digital Subscriber Line)

4 Quy định chung

4.1 Khi có chức năng hoặc thiết bị của hệ thống truyền tin báo sự cố được tích hợp vào thiết bị báo cháy (FDAD) hoặc thiết bị thông báo tại trung tâm tiếp nhận (AE) thì các chức năng hoặc thiết bị đó phải đáp ứng yêu cầu của tiêu chuẩn này.

4.2 Nếu có những chức năng khác được cung cấp thêm, ngoài các chức năng được quy định trong tiêu chuẩn này thì những chức năng được cung cấp thêm đó phải đảm bảo không phá vỡ sự tương thích với bất kỳ yêu cầu nào của tiêu chuẩn này và đáp ứng các quy định của pháp luật hiện hành khác có liên quan (nếu có),

4.3 Hệ thống và thiết bị thuộc hệ thống truyền tin báo sự cố phải đáp ứng các yêu cầu kỹ thuật và quy định của pháp luật hiện hành bao gồm việc kết nối, thiết lập và chấm dứt kết nối và truyền tải thông qua mạng điện thoại và dữ liệu công cộng và/hoặc các quy định về truyền tín hiệu qua hệ thống sóng vô tuyến, hệ thống phân phối điện hoặc hệ thống phân phối truyền hình cáp

5 Yêu cầu đối với hệ thống truyền tin báo sự cố

5.1 Yêu cầu chung

5.1.1 Nhiệm vụ của ATS là bảo đảm thông báo báo động từ FDAD được truyền tải tới ARC một cách kịp thời, chính xác. Chức năng chính của ATS là cung cấp mạng truyền tin cậy và an toàn từ giao diện của FDAD tới SPT đến giao diện của RCT tới AE để truyền tin báo động. ATS sẽ cung cấp thông tin liên lạc giữa một hoặc nhiều FDAD tại một cơ sở được giám sát và một hoặc nhiều AE của một hoặc nhiều ARC.

Ghi chú: thông báo báo động có thể bao gồm cảnh báo cháy, cảnh báo lỗi, tín hiệu giám sát, tín hiệu trạng thái tắt, tín hiệu trạng thái kiểm tra của FDAD (xem 3.1.46)

5.1.2 Cấu hình ATS phải đáp ứng các quy định sau:

a) Có tối thiểu 2 đường truyền (ATP). Trong đó có 1 đường truyền chính, một đường truyền dự phòng hoặc được sử dụng song song

b) SPT phải có giao diện mạng chính và dự phòng;

c) Phải có RCT dự phòng;

d) RCT phải có giao diện mạng chính và dự phòng;

e) phải có ATSP cho cả giải pháp ATS lưu trữ và ATS không lưu trữ

Ghi chú: Cấu hình logic ATS được trình bày tại hình A.1 Phụ lục A

5.2 Yêu cầu liên kết truyền dẫn

5.2.1 Yêu cầu chung

5.2.1.1 ATP có thể bao gồm các liên kết chuyên dụng cố định, liên kết ảo cố định hoặc liên kết chuyển mạch. Các liên kết này có thể sử dụng có thiết bị không được quy định tại Điều 6, Điều 7 của tiêu chuẩn này (xem 3.1.26) hoặc có thể bị ảnh hưởng bởi các ứng dụng khác chia sẻ liên kết truyền dẫn.

5.2.1.2 ATP có thể bao gồm:

a) Liên kết truyền dẫn được chia sẻ với các ứng dụng dữ liệu không nhằm mục đích truyền tin báo động;

b) Liên kết truyền dẫn mang các ATP khác;

c) Thiết bị từ nhà cung cấp mạng truyền của bên thứ ba, không nằm ở cơ sở được giám sát hoặc trung tâm tiếp nhận báo động và không được phân loại là ATE;

d) Thiết bị từ bên thứ ba được đặt tại cơ sở được giám sát nhưng không được phân loại là ATE.

5.2.1.3 Hiệu suất (độ tin cậy) của ATS có thể bị ảnh hưởng bởi:

a) Dữ liệu đến không mong muốn, không đúng định dạng hoặc chủ ý phá hoại tại các giao diện của SPT hoặc RCT

b) Tắc nghẽn mạng truyền dẫn do chia sẻ liên kết truyền dẫn,

c) Mạng truyền dẫn không khả dụng do thiết bị hỏng và/hoặc bảo trì.

5.2.2 Đường truyền được chia sẻ với các ứng dụng khác

Các đường truyền được chia sẻ với các ứng dụng khác phải được sắp xếp sao cho việc vận hành và bảo trì không ngăn cản ATS đáp ứng các yêu cầu của tiêu chuẩn này.

5.2.3 Thiết bị mạng truyền dẫn

Thiết bị truyền dẫn được kết nối giữa giao diện mạng truyền dẫn của SPT và giao diện mạng truyền dẫn của RCT và/hoặc MCT không phải tuân theo các yêu cầu tại Điều 6 và Điều 7 của tiêu chuẩn này.

Ghi chú 1: Ví dụ giao diện mạng tích hợp SPT bao gồm modem tương tự (analog), bộ thu phát tín hiệu DTMF, bộ điều hợp đầu cuối ISDN, mô-đun Ethernet và mô-đun radio GSM. Các công nghệ này đều có thể được sử dụng.

Ghi chú 2: Các lỗi giao diện mạng cục bộ có thể được SPT phát hiện và báo cáo cho RCT bằng cách sử dụng đường truyền truyền dẫn còn lại; tuy nhiên, không thể sử dụng giám sát giao diện để xác nhận rằng đường truyền truyền dẫn đang hoạt động.

5.2.4 Dung lượng của ATSN

5.2.4.1. ATSP sẽ phải công bố về số lượng FDAD có thể được kết nối với ATSN và đáp ứng quy định tại 5.3.2.

5.2.4.2. Bất kỳ ATP riêng lẻ nào của ATS cũng phải liên tục đáp ứng các yêu cầu về thời gian truyền quy định tại 5.3.2 trong các điều kiện sau:

a) Với tốc độ tương đương một thông báo mỗi phút từ mỗi FDAD, số lượng FDAD phải đai diện cho ít nhất 0,1% dung lượng của hệ thống và;

b) với tốc độ ít nhất 2 báo động mỗi phút tại giao diện RCT tới AE.

5.2.5 Từ chối dịch vụ

5.2.5.1 ATS sẽ tự bảo vệ mình khỏi các cuộc tấn công từ chối dịch vụ (DoS) từ mạng truyền dẫn.

5.2.5.2 Bất kỳ dạng dữ liệu hoặc tín hiệu nào nhận được từ mạng truyền dẫn cũng không được phép ngăn cản ATP thực hiện chức năng đã quy định, trừ khi lượng dữ liệu đến dẫn đến tắc nghẽn liên kết truyền dẫn. Không được phép giảm hiệu suất ATP khi vẫn còn đủ dung lượng mạng để truyền các tín hiệu do ATP truyền tải.

5.2.5.3 Bất kỳ dữ liệu độc hại nào nhận được từ giao diện mạng truyền dẫn đều không ảnh hưởng đến hoạt động của ATE (SPT, RCT hoặc MCT) hoặc hoạt động của bất kỳ giao diện mạng truyền dẫn nào khác. Điều này áp dụng ngay cả khi tốc độ dữ liệu độc hại đạt đến dung lượng của một giao diện duy nhất, khiến giao diện đó không hoạt động.

5.2.5.4 Nếu hiệu suất của ATS bị ảnh hưởng bởi một cuộc tấn công DoS, tín hiệu lỗi sẽ được tạo theo các yêu cầu giám sát và báo cáo lỗi theo quy định tại bảng 1.

Ghi chú 1: Yêu cầu này nhằm nhấn mạnh nhu cầu bảo vệ chống lại các cuộc tấn công trong đó dữ liệu hoặc tín hiệu độc hại được sử dụng để can thiệp vào hoạt động của ATE. Các cuộc tấn công này có thể được thực hiện bằng tín hiệu độc hại được thiết kế để làm suy yếu ATE hoặc bằng cách làm quá tải các thông tin liên lạc với lượng dữ liệu lớn.

Ghi chú 2: Các cuộc tấn công DoS có thể có trong bất kỳ mạng nào, ví dụ như mạng IP, mạng PSTN. Ví dụ về các cuộc tấn công như vậy là: các thiết bị cố tình làm quá tải mạng IP, các tiện ích quay số tự động để làm quá tải các phần của mạng PSTN, các thiết bị gây nhiễu để can thiệp vào thông tin liên lạc vô tuyến, v.v.

5.3 Yêu cầu hiệu suất

5.3.1 Yêu cầu chung

Hiệu suất của ATS phải được đánh giá dựa trên các tiêu chí về thời gian truyền, thời gian báo cáo, khả năng giám sát các kết nối và tính khả dụng của ATSN

5.3.2 Thời gian truyền

5.3.2.1 Thời gian truyền của ATS phải bảo đảm các yêu cầu sau:

a) Thời gian truyền trung bình phải không được vượt quá 10 s;

b) Bách phân vị thứ 95 của các lần truyền không được vượt quá 15 s;

c) Thời gian truyền lớn nhất không được vượt quá 30 s.

5.3.2.2 Bất kỳ thời gian truyền nào vượt quá thời gian truyền lớn nhất đối với mỗi sự cố, sẽ được phân loại là lỗi hệ thống với ghi chú tại 5.3.2.5.

5.3.2.3 Thời gian được đo từ thời điểm xảy ra thay đổi trạng thái hoặc thông báo báo động được trình bày để truyền tại giao diện SPT tới FDAD cho đến thời điểm trạng thái hoặc thông báo mới được báo cáo tại giao diện RCT tới AE.

5.3.2.4 Thời gian truyền áp dụng cho tất cả các thay đổi trạng thái hoặc thông báo được truyền từ FDAD qua giao diện SPT tới ATS.

Ghi chú 1: Khi giao diện SPT tới FDAD không thể truy cập được, phép đo có thể được thực hiện từ một điểm dễ truy cập hơn trước giao diện SPT với FDAD và áp dụng hiệu chỉnh thích hợp cho kết quả.

Ghi chú 2: Khi giao diện RCT tới AE không thể truy cập được hoặc khi thuận tiện hơn, phép đo có thể được thực hiện đến một điểm sau giao diện RCT tới AE và áp dụng hiệu chỉnh thích hợp cho kết quả.

Ghi chú 3: Thời gian trong FDAD và trong AE sẽ được chỉ định trong các tiêu chuẩn khác.

Ghi chú 4: Thời gian truyền bao gồm thời gian thiết lập kết nối.

5.3.2.5 Khi thời gian truyền không thể đo trực tiếp thì có thể chấp nhận được việc đo thời gian khứ hồi. Trong trường hợp này, thời gian khứ hồi phải đáp ứng các yêu cầu tại 5.3.2.1 và Bảng 1

Ghi chú 1: Thời gian truyền có thể không bằng một nửa thời gian khứ hồi.

Ghi chú 2: Thời gian khứ hồi là thời gian được đo từ khi xảy ra thay đổi trạng thái hoặc thông báo cảnh báo được trình bày để truyền tại giao diện SPT tới FDAD cho đến thời điểm tín hiệu hoặc thông báo xác nhận tích cực được trình bày tới FDAD (tại giao diện SPT tới FDAD).

5.3.3 Giám sát các kết nối

5.3.3.1 Tổng quan

Tất cả các liên kết và kết nối sau đây của ATS sẽ được giám sát và các lỗi sẽ được phát hiện, báo cáo và ghi lại:

a) Giám sát kết nối FDAD với SPT, áp dụng cho cả các giải pháp FDAD và SPT tích hợp;

b) Giám sát đầu cuối ATP;

c) Giám sát kết nối RCT với AE.

5.3.3.2 Giám sát kết nối với FDAD

Trong trường hợp xảy ra lỗi kết nối giữa FDAD và SPT, tín hiệu lỗi hoặc tín hiệu cảnh báo sẽ được tạo và truyền đến AE có liên quan và nếu có thể, đến các MCT trong thời gian quy định tại 5.3.2.

5.3.3.3 Giám sát ATS

5.3.3.3.1 Các ATP sẽ sử dụng nhiều giao diện khác nhau (ví dụ như đường truyền báo động cố định và đường truyền vô tuyến sử dụng mạng của nhà cung cấp dịch vụ di động) để kết nối SPT với các mạng truyền dẫn theo cách mà một hành động phá hoại đơn lẻ trên mạng truyền dẫn không thể khiến tất cả các ATP bị hỏng cùng lúc. Một trong các ATP, của hệ thống đường truyền kép, sẽ được xác định như là ATP chính, ATP còn lại sẽ được xác định là ATP dự phòng. Tất cả ATP sẽ được giám sát với thời gian báo cáo không được vượt quá các giá trị được quy định tại Bảng 1.

Bảng 1. Thời gian báo cáo tối đa

STT	Các lỗi được giám sát	Thời gian báo cáo tối đa
1.	ATP chính lỗi	90 s
2.	ATP chính đang hoạt động bình thường và xuất hiện lỗi tại ATP dự phòng	5h
3.	ATP dự phòng đang lỗi và ATP chính xuất hiện lỗi	90 s
4.	Tất cả các ATP lỗi cùng lúc	3 min

Ghi chú 1: Tần suất trao đổi thông báo trạng thái phải lớn hơn thời gian báo cáo trong Bảng 1 để giảm thiểu việc tạo ra báo động giả. Các thông báo trạng thái phải được mã hóa và bảo vệ chống giả mạo.

Ghi chú 2: Các lỗi giao diện mạng cục bộ có thể được SPT phát hiện và báo cáo cho RCT bằng cách sử dụng đường truyền hoạt động còn lại; tuy nhiên, việc việc sử dụng giám sát giao diện không thể được xem là một phương pháp đầy đủ để xác minh rằng đường truyền đó hoặc các đường truyền khác trong hệ thống hoàn toàn ổn định và đáng tin cậy.

5.3.3.3.2 ATS phải báo cáo tất các lỗi ATS và lỗi ATP đến AMS và cho từng loại AE5 .Tất cả các lỗi ATS sẽ được trình bày cho ATSP để có hành động thích hợp.

5.3.3.3.3 Lỗi ATS phải được SPT nhận biết và chỉ báo.

5.3.3.4 Giám sát kết nối với AE

Kết nối giữa RCT và AE sẽ được giám sát. Trong trường hợp kết nối bị lỗi, tín hiệu lỗi sẽ được ghi lại và trình bày cho AE và RCT hoặc trung tâm giám sát có liên quan. Thời gian báo cáo của tín hiệu lỗi phải đáp ứng yêu cầu tại bảng 1 về thời gian báo cáo ngắn nhất của bất kỳ ATP nào được liên kết.

5.4 Bảo đảm an toàn cho các thông báo

Thông báo sẽ không bị mất trong trường hợp mất điện hoặc bất kỳ sự kiện nào khác do SPT hoặc RCT tạo ra bên trong, chẳng hạn như đặt lại phần mềm

5.5 Xác nhận truyền báo động

Phải có biện pháp để xác nhận rằng mỗi báo động nhận được tại SPT từ FDAD và mỗi cảnh báo do ATS tạo ra đều được chuyển đến AE một cách chính xác. Điều này có thể được thực hiện bằng cách RCT sẽ gửi một thông báo xác nhận về việc báo động hoặc cảnh báo đã được chuyển đến đích theo thời gian quy định, hoặc một thông báo lỗi về sự thất bại khi chuyển tín hiệu đến đích hoặc thời gian xác nhận không bảo đảm quy định sẽ được tạo ra. Thông báo xác nhận hoặc thông báo lỗi phải được gửi đến FDAD bởi SPTvà được chỉ báo tại SPT

5.6 Cảnh báo do ATS tạo ra

5.6.1.1.1 ATS phải báo cáo tất cả các lỗi ATS và ATP đến AMS và AE.

5.6.1.1.2 Khi ATS bị lỗi, một thông báo cảnh báo sẽ được tạo ra và được truyền đến AMS và AE có liên quan và nếu có thể, đến các MCT trong thời gian được quy định tại 5.3.2.

5.6.1.1.3 Khi ATS vẫn hoạt động, lỗi đường truyền đơn sẽ được trình bày cho ATSP, nhưng có thể bị trì hoãn trình bày cho AMS khi các bên liên quan thống nhất. Độ trễ tối đa không được vượt quá 96 giờ.

Ghi chú 1 Nhà cung cấp dịch vụ truyền báo động phải ghi lại các thông báo được sử dụng để báo cáo các cảnh báo cần thiết cho AMS.

Ghi chú 2 Phương pháp báo cáo cảnh báo về tất cả các đường dẫn không thành công đến AMS phải là thông báo “lỗi đường truyền chính của ATS” và thông báo “lỗi đường truyền thay thế của ATS” và/hoặc thông báo “tất cả các đường truyền bị lỗi”. ATSP phải ghi lại phương pháp báo cáo.

Ghi chu 3 Được phép có nhiều hơn hai đường truyền.

5.6.1.1.4 Khi ATS bị lỗi, một thông báo cảnh báo sẽ được SPT truyền tới FDAD theo quy định tại Điều 6. Đối với lỗi ATP, không cần phải báo cáo cho FDAD trừ khi được chỉ định và thống nhất giữa các bên liên quan.

Ghi chú Khi báo cáo lỗi ATP đến AMS bị chậm trễ, có thể phát sinh nhầm lẫn nếu người dùng FDAD biết về lỗi ATP. Do đó, trong những trường hợp này, khuyến cáo không báo cáo lỗi ATP cho FDAD.

5.7 Tính khả dụng

5.7.1 Tổng quan

5.7.1.1 Tính khả dụng của ATP, ATS và ATSN là tỷ lệ phần trăm thời gian mà ATP, ATS và ATSN hoạt động đúng yêu cầu của tiêu chuẩn này

Ghi chú 1: Không nên nhầm lẫn giữa tính khả dụng của ATP, ATS và ATSN với tính khả dụng của mạng truyền dẫn. Để tính toán tính khả dụng của ATP và toàn hệ thống ATS, cần xem xét tính khả dụng của ba thành phần chính: SPT, mạng truyền dẫn, và RCT theo dạng nối tiếp. Nếu bất kỳ thành phần nào trong chuỗi này không hoạt động, thì tính khả dụng tổng thể sẽ bị ảnh hưởng.

Ghi chú 2: Trong tiêu chuẩn này, tính khả dụng của các ATP phải được coi là song song (xem phụ lục B).

Ghi chú 3: Tính khả dụng của ATSN được sử dụng để cung cấp chỉ báo hiệu suất của ATSN cho ATSP

5.7.1.2 Trừ khi có tình huống báo động hoặc lỗi, ATS phải được giám sát để đảm bảo tính toàn vẹn của nó. Việc giám sát cần đủ thường xuyên để đáp ứng yêu cầu về thời gian báo lỗi quy định trong Bảng 1.

5.7.1.3 Phải cung cấp bằng chứng cho thấy tính khả dụng có thể được ghi lại và có thể kiểm tra bất kỳ lúc nào.

5.7.2 Tính dự phòng/ sao chép

Khi có nhiều giao diện với ATS tại SPT hoặc tại RCT, ATS sẽ vẫn được coi là khả dụng trong trường hợp xảy ra lỗi ảnh hưởng đến một hoặc nhiều giao diện như vậy với điều kiện:

a) ít nhất một ATP tồn tại giữa một giao diện tại FDAD và một giao diện tại AE; và

b) Tất cả các giao diện phải thường xuyên được sử dụng để truyền và nhận thông báo (tin nhắn); hoặc các thông báo thường được truyền và nhận trên một giao diện chính ở mỗi đầu (SPT và RCT), nhưng trong trường hợp xảy ra lỗi, hệ thống sẽ tự động chuyển sang giao diện thay thế.

5.7.3 ATS không khả dụng

ATS sẽ được coi là không khả dụng trong khi bất kỳ các tình huống sau đây sẽ được xem xét:

a) tất cả các lỗi trong ATS, điều này sẽ ngăn chặn báo động được truyền đến các ARC dự định của nó theo yêu cầu của tiêu chuẩn này;

b) không khả dụng do bảo trì ATS, trừ khi có các thiết bị thay thế được sử dụng.

5.7.4 Thời gian xảy ra lỗi

Thời gian mà ATS được coi là không khả dụng sẽ là khoảng thời gian từ lần cuối cùng hệ thống được biết là khả dụng (tức là không có lỗi) cho đến thời điểm phát hiện lỗi, sửa chữa lỗi và xác nhận hệ thống khả dụng trở lại.

Ghi chú Lỗi do cố ý xâm phạm, làm gián đoạn hoặc phá hoại hệ thống không đưa vào để xem xét tính khả dụng của hệ thống miễn là chúng được phát hiện và báo cáo trong thời gian quy định tại Bảng 1.

5.7.5 Ghi lại tính khả dụng của ATS

5.7.5.1 Để theo dõi và xác minh hiệu suất, phải ghi lại tính khả dụng của ATP và ATS.

5.7.5.2 Khi tính khả dụng của ATS thấp hơn 99,8% trong bất kỳ khoảng thời giang 7 ngày nào phải ghi rõ trong hồ sơ tính khả dụng.

5.7.5.3 Khi tính khả dụng của ATP thấp hơn 95% trong bất kỳ khoảng thời gian 7 ngày nào, phải ghi rõ trong hồ sơ tính khả dụng.

5.7.5.4 ATSP phải có các quy trình và thủ tục để cung cấp báo cáo tính khả dụng cho các bên quan tâm nhằm mục đích duy trì mức hiệu suất yêu cầu (xem phụ lục B)

5.7.6 Tính khả dụng của ATSN

Tính khả dụng hàng năm của ATSN không được thấp hơn 99,9 %. Nếu ATSN không đáp ứng được yêu cầu trên thì sẽ ghi lại lỗi.

5.8 Bảo mật

5.8.1 Yêu cầu chung

5.8.1.1 ATSP sẽ mô tả các phương pháp để bảo vệ ATS và các thành phần của nó (ví dụ: SPT, RCT và RCT được lưu trữ) chống lại các cuộc tấn công độc hại và ảnh hưởng vô ý.

5.8.1.2 Để đảm bảo bảo mật thông tin và chống giả mạo, các kỹ thuật mật mã sẽ được sử dụng.

5.8.1.3 Khi sử dụng các thuật toán mã hóa đối xứng, độ dài khóa không được nhỏ hơn 128 bit. Khi triển khai các thuật toán khác, chúng sẽ cung cấp mức độ mạnh mật mã tương tự. Bất kỳ hàm băm nào được sử dụng sẽ phải cung cấp đầu ra tối thiểu 128 bit. Các khóa phải được thay đổi tự động và thường xuyên một cách ngẫu nhiên do hệ thống tạo ra.

5.8.1.4 Khuyến nghị sử dụng các thuật toán mật mã theo định nghĩa trong TCVN 11367 (ISO/IEC 18033). Khuyến nghị sử dụng các hàm băm theo định nghĩa trong TCVN 11816 (ISO/IEC 10118).

5.8.1.5 Các biện pháp bảo mật này sẽ áp dụng cho tất cả dữ liệu và chức năng quản lý của ATS bao gồm cấu hình từ xa, thay đổi phần mềm/firm ware của tất cả ATE.

5.8.2 Bảo mật chống giả mạo

5.8.2.1 Cần phải có biện pháp bảo vệ chống giả mạo để chống lại việc thay thế trái phép SPT bằng thiết bị giống hệt hoặc thiết bị mô phỏng dọc theo ATS.

5.8.2.2 Việc xác thực luôn yêu cầu đủ số lượng khóa để đảm bảo mỗi SPT và RCT đều có một mã khóa riêng biệt.

5.8.3 Bảo mật thông tin

Cần phải có biện pháp bảo vệ thông tin được truyền đi bởi ATS để ngăn chặn việc đọc trái phép và phát hiện việc sửa đổi trái phép thông tin được truyền đi.

5.9 Giải pháp ATS lưu trữ

5.9.1 Một RCT sẽ phải được đặt trong MARC (trong giải pháp không lưu trữ) hoặc phải được đặt tại một vị trí an toàn với giao diện mở rộng qua mạng truyền dẫn an toàn đến AMS tại MARC (trong giải pháp lưu trữ).

5.9.2 Trong giải pháp RCT lưu trữ, khi giao diện giữa phần lưu trữ của RCT (RCT-H) và phần ARC của RCT (RCT-A, được đặt tại MARC) được mở rộng qua mạng truyền dẫn, hiệu suất của liên kết giao diện truyền dẫn mở rộng, bao gồm RCT-A phải không thấp hơn quy định tại 5.3 và 5.7

Ghi chú: Điều này có nghĩa là hiệu suất của giao diện mở rộng (mạng truyền dẫn) phải đảm bảo để không làm giảm hiệu suất của ATS.

5.9.3 Trong giải pháp RCT lưu trữ, cả RCT-H và RCT-A phải đáp ứng các yêu cầu tại Điều 7 tiêu chuẩn này.

5.9.4 RCT-A là một phần của ATS và việc giám sát toàn diện đầu – cuối (End-to-End của ATS) (xem Hình A.3 Phụ lục A) là trách nhiệm của ATSP. ATSP phải đảm bảo rằng toàn bộ quá trình truyền tín hiệu

từ nguồn đến đích hoạt động đúng cách và đáp ứng các yêu cầu của tiêu chuẩn này.

5.9.5 Giao diện mở rộng giữa RCT và AMS là trách nhiệm của ATSP. ATSP phải đảm bảo rằng kết nối giữa RCT và AMS qua giao diện mở rộng hoạt động ổn định, bảo mật và tuân thủ các yêu cầu của tiêu chuẩn.

5.9.6 Nên sử dụng giao diện mở rộng nhân đôi (duplicated extended interface) tới AMS

5.10 Tài liệu hướng dẫn

Các ATSP phải xây dựng, duy trì tài liệu đầy đủ về lập kế hoạch, lắp đặt, đưa vào vận hành, bảo dưỡng và vận hành ATS. Hướng dẫn ATE phải được cấu trúc để phân loại các mức truy cập khác nhau của người dùng.

6 Yêu cầu đối với thiết bị thu phát tại cơ sở giám sát (SPT)

6.1 Yêu cầu chức năng của SPT

6.1.1 Yêu cầu chung

6.1.1.1 SPT phải có khả năng xử lý các tín hiệu sau sau đây:

a) Nhận tín hiệu báo động từ FDAD;

b) Nhận tín hiệu cảnh báo lỗi từ mạng truyền dẫn;

c) Nhận tín hiệu xác nhận từ RCT.

d) Truyền tín hiệu báo động tới RCT;

e) Truyền tín hiệu xác nhận tới FDAD;

f) Truyền tín hiệu cảnh báo đến RCT, bao gồm: lỗi ATP; lỗi kết nối giữa SPT với FDAD; lỗi nguồn điện (chính và dự phòng) SPT.

6.1.1.2 Các chỉ báo và/hoặc dạng đầu ra của SPT không được bị loạn khi tiếp nhận một hoặc nhiều tín hiệu đồng thời quy định tại 6.1.1.1

6.1.1.3 SPT có thể đặt rời hoặc tích hợp trong FDAD.

6.1.2 Trạng thái và chỉ báo trạng thái của SPT

6.1.2.1 SPT phải có khả năng chỉ báo một cách tường minh những trạng thái chức năng sau:

6.1.2.1.1 Trạng thái báo động khi nhận tín hiệu báo động từ FDAD, gồm các tín hiệu sau:

a) tín hiệu báo động cháy từ FDAD (chức năng bắt buộc);

b) tín hiệu cảnh báo-lỗi từ FDAD (chức năng tùy chọn);

c) tín hiệu trạng thái giám sát từ FDAD (chức năng tùy chọn);

d) tín hiệu trạng thái tắt từ FDAD (chức năng tùy chọn);

e) tín hiệu trạng thái kiểm tra từ FDAD (chức năng tùy chọn).

6.1.2.1.2 Khi một trong các lỗi sau được chỉ ra:

f) lỗi kết nối giữa SPT và FDAD;

g) lỗi trong mạng truyền báo động;

h) lỗi trong SPT (ví dụ như lỗi lỗi nguồn điện chính và dự phòng)

6.1.2.1.3 Khi SPT ở trạng thái tĩnh lặng: SPT được cấp nguồn bởi một nguồn điện phù hợp mà không có trạng thái chức năng nêu tại 6.1.2.1.1 và 6.2.1.2 được chỉ báo.

6.1.2.2 Chỉ báo trạng thái của SPT

6.1.2.2.1 Trạng thái của SPT phải được chỉ báo bằng đèn báo chỉ thị đặt rời và/ hoặc một trường trên màn hình chữ số. Đèn chỉ báo phải lóe sáng khi SPT nhận biết được trạng thái và hiển thị ổn định khi SPT nhận được sự phản hồi xác nhận từ RCT rằng tín hiệu đó đã được tiếp nhận một cách đúng đắn.

6.1.2.2.2 Có thể chỉ báo bổ sung bằng âm thanh từ còi báo hoặc thiết bị tương tự. Chỉ thị âm thanh không được tắt một cách tự động, chỉ có thể tắt được ở mức truy cập 1 hoặc 2. Sau khi được tắt, chỉ thị âm thanh phải tiếp tục phát khi có một báo động hoặc một báo lỗi khác tiếp tục được phát hiện.

6.1.2.2.3 Nếu có các chỉ báo bổ trợ cho các chỉ báo bắt buộc, thì những chỉ báo bổ trợ đó không được gây ra sự hiểu ngược hoặc hiểu sai.

6.1.2.2.4 SPT sẽ ưu tiên cao nhất xử lý và truyền tín hiệu báo động nhận được từ FDAD so với các tín hiệu khác. Trong các tín hiệu báo động từ FDAD, tín hiệu báo động cháy sẽ được ưu tiên cao nhất, tiếp theo là tín hiệu báo động lỗi. Những chỉ báo của các trạng thái khác phải được loại bỏ khi SPT nhận được tín hiệu báo động ưu tiên và có thể phát hiện ra những chỉ báo đó bằng một thao tác thủ công ở mức truy cập 1.

6.1.2.2.5 SPT phải tự động hủy bỏ (ngừng báo cáo và hiển thị) trạng thái khi trạng thái báo động đã được đặt lại tại FDAD hoặc lỗi đã được khắc khục. Việc đặt lại trạng thái báo động không được yêu cầu bất kỳ can thiệp thủ công nào. Sau khi đặt lại, việc chỉ báo các trạng thái báo động, báo lỗi phải chính xác, tương ứng với bất kỳ tín hiệu nào nhận được.

6.1.3 Chế độ hoạt động khi nhận tín hiệu báo động từ FDAD

6.1.3.1 Khi SPT nhận được báo động, SPT sẽ bảo mật và xác nhận đã nhận báo động cho FDAD. SPT sẽ chuyển báo động đến RCT. Tất cả các thông báo báo động phải gồm dấu ngày và giờ chính xác theo độ phân giải quy định tại 6.1.14.4.

6.1.3.2 SPT phải có bộ nhớ không mất dữ liệu để bảo vệ thông báo báo động trong trường hợp mất điện hoặc ATS bị lỗi; các báo động đã lưu trữ sẽ được truyền đi khi tình trạng lỗi được xóa.

6.1.4 Báo cáo lỗi ATS cho FDAD

6.1.4.1 Thời gian báo cáo lỗi ATS cho FDAD của SPT phải không quá 180 s.

Ghi chú: Khi FDAD và SPT mất kết nối, có thể sử dụng kết nối độc lập giữa FDAD và SPT để truyền tín

hiệu báo lỗi kết nối đã tới FDAD

6.1.5 Giao diện tới FDAD

6.1.5.1 Các kết nối với FDAD phải được SPT giám sát theo quy định tại 6.2.3.2. Thời gian tối đa để phát hiện và tạo ra lỗi giao diện SPT tới FDAD phải không vượt quá 90 s.

6.1.5.2 Có thể sử dụng bất kỳ loại giao diện nào của SPT tới FDAD, miễn là đáp ứng yêu cầu của tiêu chuẩn này. Nhà sản xuất phải nêu trong tài liệu kỹ thuật cụ thể loại giao diện của SPT tới FDAD.

Ghi chú: Để cho phép tương thích giữa các nhà sản xuất khác nhau, Phụ lục F quy định hai loại giao diện nối tiếp và song song có thể có giữa FDAD và SPT.

6.1.6 Giám sát giao diện mạng truyền dẫn

Nếu SPT có chức năng giám sát giao diện mạng và báo cáo lỗi cho FDAD và/hoặc RCT, tài liệu của nhà sản xuất sẽ mô tả cách thực hiện việc này.

Ghi chú: Việc triển khai giám sát giao diện mạng và báo cáo lỗi không bắt buộc. Tuy nhiên, điều này có thể hữu ích giúp xác định và phân tích nguyên nhân gây ra lỗi đường truyền cho ATSP.

6.1.7 Cảnh báo do SPT tạo ra

SPT phải có khả năng tạo và truyền đến RCT các thông báo cảnh báo gồm:

a) Lỗi nguồn điện SPT chính và khôi phục;

b) Lỗi nguồn điện SPT dự phòng và khôi phục;

c) lỗi ATP chính và khôi phục;

d) lỗi ATP dự phòng và khôi phục;

đ) lỗi kết nối với FDAD và khôi phục.

6.1.8 Yêu cầu về cấp quyền truy cập logic (xem phục lục C)

6.1.8.1 Truy cập logic vào các chức năng phải đáp ứng các quy định sau:

a) Truy cập vào các chức năng yêu cầu mức truy cập 2, 3 và 4 phải yêu cầu ủy quyền bằng khóa.

b) Truy cập ở mức 3 phải được ủy quyền bởi người dùng có quyền truy cập mức 2. Quyền truy cập ở mức 4 phải được ủy quyền bởi người dùng có quyền truy cập mức 3. Điều này có thể đạt được bằng cách ủy quyền một lần như một phần của thỏa thuận mức dịch vụ.

c) Có thể đạt được quyền truy cập ở mức 2, 3 và 4 bằng cách cung cấp quyền tương đương với 1.000.000 khóa khác nhau.

6.1.8.2 Trong trường hợp có thể cố gắng truy cập nhiều hơn 3 lần trong khoảng thời gian 60 giây, SPT phải có khả năng trì hoãn các lần thử lặp lại. Sau lần thử thứ ba, mỗi lần thử tiếp theo sẽ bị ngăn chặn trong tối thiểu 90 giây.

6.1.8.3 Nếu có khóa mặc định từ nhà sản xuất, sẽ không thể hoàn tất việc cấu hình SPT để đưa vào hoạt động nếu không thay đổi các khóa này, ví dụ như trong quá trình cài đặt. Sẽ không thể đọc được bất kỳ khóa nào cung cấp quyền truy cập ở mức 2, 3 hoặc 4.

6.1.9 Bảo mật chống giả mạo

Nhà sản xuất phải cung cấp phương pháp được sử dụng để đảm bảo quy định tại 5.8.2

6.1.10 Bảo mật thông tin

Nhà sản xuất phải cung cấp phương pháp được sử dụng để đảm bảo quy định tại 5.8.3

6.1.11 Truy cập từ xa

Truy cập từ xa vào SPT phải đáp ứng các yêu cầu bảo mật tối thiểu như yêu cầu đối với việc truyền báo động quy định tại Điều 5 và Điều 8 của tiêu chuẩn này.

6.1.12 Tải lên và tải xuống phần mềm và chương trình cơ sở (firmware)

6.1.12.1 Khi chức năng tải lên và tải xuống được cung cấp, việc tải lên và tải xuống phần mềm vào SPT chỉ được phép thực hiện bởi người dùng có mức độ truy cập phù hợp, như được định nghĩa tại phụ lục C và quy định tại 6.1.8

6.1.12.2 Phần mềm được thay thế bằng quá trình tải xuống phần mềm phải được lưu trữ trước khi thay thế. Nếu mất kết nối hoặc lỗi truyền tải khác làm gián đoạn quá trình tải xuống, phiên bản phần mềm đầy đủ chức năng cuối cùng phải được khôi phục và SPT sẽ hoạt động trở lại như trước khi tải xuống không thành công.

Ghi chú: Ví dụ về quy trình tải xuống: tải xuống phần mềm, kiểm tra và xác thực tải xuống, kích hoạt phần mềm đã tải xuống.

6.1.13 Lưu trữ các thông số

Quá trình cấp nguồn lại (ví dụ sau khi mất điện và được khôi phục lại) hoặc khởi động lại SPT sẽ không dẫn đến mất bất kỳ dữ liệu riêng nào. SPT phải trở lại hoạt động bình thường.

6.1.14 Ghi nhật ký sự kiện

6.1.14.1 SPT phải có khả năng ghi nhớ các sự kiện được quy định tại bảng 2.

Ghi chú: SPT không nhất thiết phải có chức năng của tất cả các sự kiện được ghi lại tại bảng 2

6.1.14.2 Phương tiện được ghi lại các sự kiện phải có khả năng ghi nhớ tối thiểu 1000 sự kiện, và được bảo vệ chống lại việc xóa hoặc thay đổi nội dung một cách vô tình hoặc cố ý. Bộ nhớ phải có độ bền tối thiểu 30 ngày sau khi SPT mất điện.

6.1.14.3 Khi SPT là một phần tích hợp của FDAD, nhật ký có thể được chia sẻ với điều kiện dung lượng bộ nhớ và độ bền của các sự kiện SPT đáp ứng các yêu cầu tại 6.1.14.2.

6.1.14.4 Ngoài các sự kiện, nhật ký phải ghi lại cả thời gian và ngày mà sự kiện xảy ra. Độ phân giải thời

gian phải tối thiểu là 71 giây (các sự kiện được phân biệt với nhau cách nhau ít nhất 71 giây). Thời gian được ghi lại phải chính xác so với giờ chuẩn quốc tế (UTC) với sai số không quá ±5 giây. SPT phải cung cấp phương pháp để điều chỉnh ngày và giờ, cho phép đồng bộ hóa thiết bị với thời gian chính xác.

6.1.14.5 SPT phải ghi lại tất cả các sự kiện khác nhau. Với các sự kiện lặp đi lặp lại giống nhau trong vòng 12 giờ, chỉ cần ghi lại sự kiện đầu tiên và cuối cùng, đồng thời ghi rõ số lần lặp lại.

6.1.14.6 Việc truy cập vào SPT phải bao gồm nhận dạng người dùng

Bảng 2 - Sự kiện cần ghi của SPT

STT	Sự kiện cần ghi
1.	Thông báo báo động từ FDAD
2.	Xác nhận thông báo từ RCT
3.	Xác nhận thông báo báo động không thành công hoặc vượt quá thời gian chờ xác nhận thông báo báo động từ RCT
4.	Nguồn điện chính SPT bị lỗi và khôi phục
5.	Nguồn điện dự phòng SPT bị lỗi và khôi phục
6.	Lỗi kết nối FDAD với SPT và khôi phục
7.	Lỗi ATP và khôi phục
8.	Lỗi ATS và khôi phục
9.	Lỗi giao diện SPT với mạng truyền dẫn và khôi phục
10.	Thay đổi cấu hình của SPT
11.	Bật nguồn hoặc thiết lập lại SPT
12.	Bất kỳ thay đổi nào đối với phần mềm SPT
13.	Thay đổi thủ công ngày và giờ
14.	Truy cập vào SPT ở mức truy cập 2, 3 hoặc 4.

6.2 Yêu cầu thiết kế

6.2.1 Yêu cầu chung và công bố của nhà sản xuất

6.2.1.1 SPT phải đáp ứng quy định tại 6.2 đối với các công nghệ liên quan được sử dụng. Để hỗ trợ cho quá trình kiểm tra thiết kế, nhà sản xuất phải công bố bằng văn bản rằng:

6.2.1.1.1 Thiết kế đã được thực hiện phù hợp với một hệ thống quản lý chất lượng có tích hợp một tập hợp các nguyên tắc để thiết kế tất cả các bộ phận của SPT (ví dụ như ISO 9001);

6.2.1.1.2 Các linh kiện của SPT đã được lựa chọn cho mục đích xác định trước và dự kiến vận hành trong phạm vi chỉ tiêu kỹ thuật của nó nếu các điều kiện môi trường bên ngoài vỏ bọc của SPT phù hợp với cấp 3k5 theo TCVN 7921-3-3.

6.2.2 Hồ sơ

6.2.2.1 Nhà sản xuất phải chuẩn bị hồ sơ về lắp đặt và hướng dẫn sử dụng. Những hồ sơ đó cùng với SPT phải được cung cấp cho đơn vị thử nghiệm được chấp nhận. Ít nhất, hồ sơ phải bao gồm những phần sau:

6.2.2.1.1 Một bản mô tả chung về thiết bị, bao gồm danh sách của:

a) Các chức năng tùy chọn của tiêu chuẩn này;

b) Các chức năng liên quan đến các quy định về thiết bị, hệ thống báo cháy hiện hành, và

c) Các chức năng không được yêu cầu bởi tiêu chuẩn này.

6.2.2.1.2 Các mô tả thông số kỹ thuật của đầu vào và đầu ra của SPT, đủ để cho phép thực hiện đánh giá về cơ học, điện, và tính tương thích của phần mềm với FDAD, bao gồm khi có liên quan:

a) Các yêu cầu về nguồn điện đảm bảo cho hoạt động theo khuyến cáo (bao gồm cả nguồn chính và dự phòng);

b) Số lượng nhiều nhất của FDAD, các vùng và/hoặc các điểm trên một SPT.

c) Các loại giao diện FDAD là SPT phù hợp;

d) Loại RCT mà SPT phù hợp (khả năng tương thích);

đ) Chế độ hoạt động (lưu trữ và chuyển tiếp và/hoặc chuyển tiếp;

e) Cách thức giám sát giao diện mạng truyền dẫn;

g) Định mức điện (điện áp, dòng điện, tần số, công suất) lớn nhất và nhỏ nhất cho mỗi tín hiệu đầu vào và đầu ra;

h) Thông tin về các tham số truyền thông tin (tốc độ truyền dữ liệu, phương thức mã hóa, giao thức, dạng tín hiệu…) được sử dụng trên mỗi đường truyền dẫn;

i) Các thông số khuyến cáo về dây dẫn cho mỗi đường truyền dẫn;

k) Các thông số định mức của cầu chì (dòng điện định mức, dòng cắt, điện áp...)

6.2.2.1.3 Các thông tin về lắp đặt, bao gồm

a) Tính phù hợp cho việc sử dụng ở các điều kiện môi trường khác nhau;

b) Làm sao để đáp ứng được các yêu cầu nêu trong 6.2.3.

d) Hướng dẫn lắp đặt,

đ) Các hướng dẫn về đấu nối đầu vào và đầu ra;

6.2.2.1.4 Hướng dẫn việc cấu hình và chạy thử.

6.2.2.1.5 Hướng dẫn vận hành.

6.2.2.1.6 Thông tin về khai thác và bảo trì.

6.2.2.1.7 Phương pháp và mô tả thử nghiệm để xác minh hiệu suất, tính khả dụng của ATS như quy định tại Điều 6 tiêu chuẩn này.

6.2.2.2 Nhà sản xuất phải chuẩn bị hồ sơ thiết kế, những hồ sơ này phải được cung cấp cho đơn vị thử nghiệm được chấp nhận cùng với SPT. Hồ sơ này phải bao gồm các bản vẽ, danh mục các bộ phận, sơ đồ khối, sơ đồ mạch và một bản mô tả chức năng, đảm bảo chi tiết đến mức có thể kiểm tra được sự phù hợp so với tiêu chuẩn này và có thể đưa ra được đánh giá chung của thiết kế phần điện và phần cơ.

6.2.3 Các yêu cầu thiết kế phần cơ

6.2.3.1 Vỏ bọc của SPT phải có kết cấu chắc chắn, phù hợp với phương pháp lắp đặt được khuyến cáo trong hồ sơ thiết kế. Ít nhất nó phải đảm bảo cấp chống xâm nhập IP 30 theo TCVN 4255 (IEC 60529) ở mức truy cập 2

6.2.3.2 SPT có thể được đặt trong từ hai vỏ bọc trở lên. Nếu hồ sơ thiết kế trình bày các vỏ bọc có thể được lắp đặt ở những vị trí phân tán trong phạm vi mặt bằng, thì tất cả các nút ấn thủ công và đèn chỉ báo bắt buộc phải được đặt trên một vỏ bọc hoặc trên các vỏ bọc được công bố là chỉ thích hợp cho việc lắp đặt liền kề nhau.

6.2.3.3 Mọi nút ấn thủ công và đèn tín hiệu nhấp nháy phải được dán nhãn rõ ràng để thể hiện mục đích của chúng. Các thông tin phải đảm bảo nhìn thấy được ở khoảng cách 0,8 m trong điều kiện cường độ sáng môi trường từ 100 lx đến 500 lx.

6.2.3.4 Các vị trí đấu nối cho đường truyền dẫn và cầu chì phải được dán nhãn rõ ràng.

6.2.4 Các yêu cầu thiết kế phần điện và thiết kế khác

6.2.4.1 SPT phải được cấp nguồn từ 2 nguồn điện độc lập khác nhau. Trong đó nguồn điện chính lấy điện từ điện sinh hoạt, nguồn điện còn lại là nguồn dự phòng có thể bằng nguồn điện của hệ thống báo cháy hoặc bằng nguồn điện riêng. Nguồn điện cho SPT phải đáp ứng các quy định tại TCVN 7568-4 (ISO 7240-4). Dung lượng của ắc quy dự phòng phải bảo đảm ít nhất 24 h cho SPT hoạt động ở chế độ tĩnh và **1 h** ở chế độ báo động.

6.2.4.2 Có thể sử dụng một ATP để phát tín hiệu về một lỗi trên ATP khác.

6.2.4.3 Nếu hồ sơ của nhà sản xuất cho thấy một SPT được bố trí nằm trong nhiều hơn 1 vỏ bọc lắp đặt ở những vị trí tách biệt thì phải quy định và cung cấp phương tiện để đảm bảo sự ngắn mạch hoặc đứt đường truyền dẫn giữa các vỏ bọc bố trí phân tán bất kỳ không ảnh hưởng đến nhiều hơn 1 chức năng trong khoảng thời gian lớn hơn 90 s tính từ khi xảy ra lỗi

6.2.4.4 Nếu SPT được thiết kế để sử dụng cùng thiết bị cấp nguồn được đặt trong 1 vỏ bọc tách rời thì phải có một cách thức phối hợp cho ít nhất 2 đường truyền dẫn đến nguồn cấp điện, sao cho nếu một trong số đường truyền dẫn đó bị ngắn mạch hoặc bị đứt thì việc cấp nguồn đến SPT vẫn được đảm bảo.

6.2.4.5 Sự chuyển đổi từ các nguồn cấp điện chính sang nguồn điện dự phòng phải không được làm thay đổi bất kỳ chỉ báo nào và/hoặc tình trạng đầu ra nào, ngoại trừ các chỉ báo hoặc tình trạng đầu ra liên quan

đến nguồn cấp.

6.2.4.6 Nếu SPT có một quy định về ngắt kết nối hoặc điều chỉnh nguồn chính hoặc nguồn điện dự phòng, thì chỉ có thể thực hiện được việc này ở mức truy cập 3 hoặc 4.

6.2.5 Khả năng tiếp cận đến các chỉ báo và các điều khiển (xem phục lục C)

6.2.5.1 Sự phân bổ chức năng cho một mức truy cập phải phòng ngừa được việc truy cập vào một mức truy cập có số hiệu cao hơn, nhưng cho phép truy cập vào vào một mức truy cập có số thấp hơn. Các nút ấn thủ công và các chức năng khác phải được nhóm lại theo mức truy cập thích hợp như quy định trong tiêu chuẩn này. Phải áp dụng những quy định sau:

6.2.5.2 Mọi chỉ báo bắt buộc phải nhìn thấy được ở mức truy cập 1 không cần có sự can thiệp thủ công trước (ví dụ như phải mở thiết bị),

6.2.5.3 Các nút ấn thủ công mức truy cập 1 phải tiếp cận được mà không cần có quy trình đặc biệt.

6.2.5.4 Các chỉ báo và các nút ấn thủ công có tính bắt buộc ở mức truy cập 1 còn phải có thể tiếp cận được ở mức truy cập 2.

6.2.5.5 Việc xâm nhập vào mức truy cập 2 phải bị hạn chế bởi một quy trình đặc biệt.

6.2.5.6 Việc xâm nhập vào mức truy cập 3 phải bị hạn chế bởi một quy trình đặc biệt, khác với quy trình đã áp dụng cho mức truy cập 2.

6.2.5.7 Việc xâm nhập vào mức truy cập 4 phải bị hạn chế bởi phương tiện đặc biệt không phải là một phần của SPT.

6.2.6 Các chỉ báo

6.2.6.1 Chỉ báo bằng các đèn tín hiệu nhấp nháy

6.2.6.1.1 Chỉ báo bắt buộc từ các đèn tín hiệu nhấp nháy phải nhìn thấy được trong điều kiện môi trường bình thường có cường độ ánh sáng đến 500 lx ở mọi góc nhìn, lên đến 22,5° theo một đường thẳng đi qua đèn tín hiệu và vuông góc với bề mặt lắp đặt đèn đó

- ở khoảng cách 3 m đối với các chỉ báo chung về trạng thái chức năng,

- ở khoảng cách 3 m đối với chỉ báo về cung cấp nguồn điện,

- ở khoảng cách 0,8 m đối với các chỉ báo khác.

6.2.6.1.2 Đối với các chỉ báo lóe sáng, thì cả chu kì bật (on-period) và chu kì tắt (off-period) phải kéo dài không ít hơn 0,25 s, và các tần số phát chớp sáng phải không thấp hơn

a) 1 Hz đối với các ở chỉ báo báo động cháy,

b) 0,2 Hz đối với các ở chỉ báo trạng thái còn lại.

6.2.6.1.3 Màu sắc của các chỉ báo chung và chỉ báo cụ thể từ đèn tín hiệu nhấp nháy phải theo quy định sau:

a) Mầu đỏ dùng cho chỉ báo về các báo động cháy,

b) Mầu vàng dùng cho chỉ báo trạng thái còn lại,

c) Mầu xanh dùng cho chỉ báo rằng SPT đang được cấp nguồn điện.

6.2.6.2 Chỉ báo bằng âm thanh.

6.2.6.2.1 Mức âm thanh nhỏ nhất ở khoảng cách 1 m so và trong môi trường yên tĩnh phải là:

a) 60 dB (thang A) đối với các hiển thị báo cháy, và 50 dB (thang A) đối với các hiển thị cảnh báo lỗi hoặc

b) 85 dB (thang A) đối với các hiển thị báo cháy, và 70 dB (thang A) đối với các hiển thị cảnh báo lỗi.

Ghi chú 1: Việc lựa chọn bộ chỉ báo bằng âm thanh a) hoặc b) phụ thuộc vào khu vực lắp đặt SPT.

Ghi chú 2: Mức âm thanh phải được đo trong các điều kiện không có sự dội lại của âm thanh.

6.2.6.3 Chỉ báo trên màn hình chữa, số

6.2.6.3.1 Nếu một màn hình chữ-số có các thành phần hoặc phân đoạn, thì phải đảm bảo một trong số đó bị lỗi cũng không ảnh hưởng đến việc diễn giải các thông tin được hiển thị.

6.2.6.3.2 Các màn hình chữ-số được dùng cho những chỉ báo bắt buộc thì ít nhất phải có một cửa sổ phân biệt được rõ ràng, có thể chứa ít nhất là 2 trường được xác định rõ.

6.2.6.3.3 Nếu mục đích của mỗi trường hiển thị không nằm trong thông tin được thể hiện thì trường hiển thị đó phải được dán nhãn rõ ràng.

6.2.6.3.4 Tiếp theo sự hiển thị của một chỉ báo mới về đám cháy hoặc lỗi, chỉ báo bắt buộc trên một màn hình chữ-số phải được nhìn thấy rõ trong khoảng thời gian ít hơn 1 h hoặc trong khoảng thời gian duy trì của nguồn điện dự phòng, ở khoảng cách 0,8 m trong điều kiện ánh sáng ở môi trường bình thường có cường độ từ 5 lx đến 500 lx và theo bất kì góc nhìn nào tính từ tia vuông góc với mặt phẳng của màn hình

a) Đến 22,5° khi nhìn từ mỗi cạnh bên

b) Đến 15° khi nhìn từ phía trên và phía dưới

c) Tiếp sau khoảng thời gian ít hơn 1 h hoặc trong khoảng thời gian duy trì của nguồn điện dự phòng, các chỉ báo phải nhìn rõ được trong điều kiện cường độ ánh sáng từ 100 lx đến 500 lx ở khoảng cách và góc nhìn như đã nêu trên. Phải đảm bảo cho phép điều chỉnh lại khả năng nhìn rõ trong điều kiện cường độ ánh sáng từ 5 lx đến 100 lx bằng thao tác vận hành thủ công ở mức truy cập 1.

6.2.6.3.5 Đối với chỉ báo báo trên màn hình chữ-số không cần thiết phải sử dụng các mầu sắc khác nhau. Tuy nhiên nếu các mầu khác nhau được sử dụng cho các chỉ báo khác nhau, thì phải tuân theo quy định về mầu sắc tại 6.2.6.1.3.

6.3 Những yêu cầu thiết kế bổ sung đối với SPT điều khiển bằng phần mềm

6.3.1 Những yêu cầu chung và công bố của nhà sản xuất

SPT có thể có các bộ phận được điều khiển bằng phần mềm để thỏa mãn các yêu cầu của tiêu chuẩn

này. Trong trường hợp đó, SPT phải phù hợp với các yêu cầu tại 6.3 nếu liên quan đến công nghệ được sử dụng.

Ghi chú: Các bộ phận điều khiển bằng phần mềm có thể được cung cấp bởi bên thứ 3 không phải là nhà sản xuất SPT miễn là đáp ứng yêu cầu của tiêu chuẩn này. Trong trường hợp này, các sản phẩm từ bên thứ 3 được thiết kế và sản xuất cho SPT phải được lưu hồ sơ đầy đủ, các nhà sản xuất các bộ phận điều khiển này có trách nhiệm bảo đảm rằng mỗi bộ phận phải tin cậy và phù hợp để SPT đáp ứng yêu cầu tại tiêu chuẩn này. Có thể coi độ tin cậy đảm bảo chứng minh được nếu các bộ phận đó luôn có sẵn trên thị trường và đã được đánh giá đạt chất lượng trong thời gian tương đối (ví dụ≥ 1 năm). Giao diện với những ứng dụng chính phải rõ ràng và được mô tả một cách tổng hợp và hồ sơ này phải luôn sẵn có để cung cấp cho đơn vị được phép thử nghiệm.

6.3.2 Hồ sơ về phần mềm

6.3.2.1 Nhà sản xuất phải chuẩn bị hồ sơ cung cấp thông tin tổng thể về thiết kế của phần mềm, những hồ sơ này phải được cung cấp cho đơn vị thử nghiệm được chấp nhận cùng với SPT. Hồ sơ này phải đảm bảo chi tiết đến mức thiết kế có thể được kiểm tra được về sự phù hợp với tiêu chuẩn này.

6.3.2.2 Nhà sản xuất phải chuẩn bị và duy trì hồ sơ thiết kế chi tiết. Không cần phải cung cấp hồ sơ này cho đơn vị thử nghiệm được chấp nhận, nhưng phải sẵn có để kiểm tra theo cách có tính đến việc tôn trọng các quyền về bảo mật của nhà sản xuất

6.3.3 Thiết kế phần mềm

Để đảm bảo độ tin cậy của SPT, phần mềm phải được thiết kế để tránh xảy ra tình trạng khóa chết (deadlock) trong luồng chương trình.

6.3.4 Giám sát chương trình

6.3.4.1 Quá trình chạy của một chương trình phải được giám sát. Phương tiện theo dõi phái phát tín hiệu về một lỗi hệ thống nếu các đoạn chương trình liên quan đến các chức năng chính của chương trình không được chạy trong khoảng thời gian giới hạn 100 s. Thiết bị giám sát phải có cơ sở thời gian độc lập với cơ sở thời gian của hệ thống được giám sát.

6.3.4.2 Một lỗi nào đó khi chạy chương trình của hệ thống theo dõi không được cản trở việc thực hiện chức năng của phương tiện theo dõi cũng như việc phát tín hiệu về một cảnh báo lỗi.

Ghi chú: Chương trình là một phần mềm cần cho SPT thực hiện các chức năng bắt buộc (bao gồm cả các tùy chọn). Cần phải theo dõi quá trình chạy toàn bộ chương trình; việc này có thể bao gồm cả những phần mềm chạy trên nhiều bộ xử lý và phần mềm trên các bộ phận mà nhà sản xuất mua về. Nhà sản xuất và đơn vị được phép thử nghiệm có trách nhiệm thỏa thuận về mức độ cần thiết của việc theo dõi, nhưng trong trường hợp của một mô đun màn hình chữ-số, việc đọc lại được dữ liệu được ghi lên mô đun từ chính bản thân màn hình cũng có thể được coi là dù để kiểm tra thông thường.

6.3.5 Lưu các chương trình và dữ liệu

6.3.5.1 Tất cả các mã chạy chương trình và dữ liệu cần thiết đảm bảo cho sự phù hợp với tiêu chuẩn này phải được lưu giữ trong một bộ nhớ đảm bảo cho phép hoạt động tin cậy một cách liên tục và không cần phải bảo trì trong khoảng thời gian ít nhất là 10 năm.

6.3.5.2 Chương trình phải được lưu giữ trong một bộ nhớ không khả biến chỉ cho phép ghi vào đó ở mức

truy cập 4. Từng thiết bị nhớ phải phân biệt rõ ràng để những nội dung của những thiết bị nhớ đó có thể được tham chiếu duy nhất đến hồ sơ về phần mềm.

6.3.5.3 Đối với các dữ liệu vị trí riêng, phải áp dụng những yêu cầu sau.

6.3.5.3.1 Việc thay đổi dữ liệu vị trí riêng chỉ cho phép thực hiện ở mức truy cập 3 hoặc 4.

6.3.5.3.2 Việc thay đổi dữ liệu vị trí riêng không được ảnh hưởng gì đến cấu trúc của chương trình.

6.3.5.3.3 Nếu được lưu giữ trong bộ nhớ khả biến, thì phải có giải pháp để bảo vệ để phòng mất nguồn điện bằng một nguồn năng lượng dự phòng, chỉ có thể tách rời nguồn dự phòng đó ra khỏi bộ nhớ ở mức truy cập 4 và nguồn dự phòng đó phải đảm bảo duy trì được bộ nhớ trong khoảng thời gian ít nhất là hai tuần.

6.3.5.3.4 Nếu được lưu giữ trong bộ nhớ đọc-ghi, thì phải có cơ chế để ngăn chặn việc ghi vào bộ nhớ trong quá trình chạy bình thường ở mức truy cập 1, đảm bảo để các nội dung của bộ nhớ được bảo vệ khi xảy ra một lỗi trong quá trình chạy chương trình.

6.3.5.3.5 Dữ liệu vị trí riêng phải được cung cấp một tham chiếu về phiên bản và nó phải được nâng cấp mỗi khi thực hiện thay đổi một tập hợp thông số.

6.3.5.3.6 Tham chiếu về phiên bản của dữ liệu vị trí riêng phải có thể xác định được ở mức truy cập 3.

6.3.6 Giám sát nội dung bộ nhớ

Các nội dung của những bộ nhớ có chứa dữ liệu vị trí riêng phải được tự động kiểm tra trong khoảng giãn cách thời gian không quá 1 h. Phương tiện kiểm tra phải phát tín hiệu về lỗi hệ thống nếu phát hiện ra một xung đột về nội dung lưu giữ trong bộ nhớ.

6.4 Yêu cầu về ghi nhãn

SPT phải được ghi nhãn bằng phương pháp bảo đảm dễ đọc, bền vững và không gây nhầm lẫn. Các thông tin ghi nhãn phải thể hiện các nội dung sau:

- Tên hoặc nhãn hiệu của nhà sản xuất;

- Các loại FDAD được SPT hỗ trợ;

- Số hiệu về loại hoặc ký hiệu khác của SPT.

Phải có thể xác định được một mã hoặc số hiệu phân biệt về chu kỳ sản xuất (thời điểm sản xuất) của SPT ở mức truy cập 2.

7 Yêu cầu đối với thiết bị thu phát tại trung tâm tiếp nhận (RCT)

7.1 Yêu cầu chung

7.1.1 Chức năng của RCT là giám sát ATS; nhận, chuyển tiếp thông báo cảnh báo và thông báo báo động đến một hoặc nhiều AE và gửi xác nhận đến các SPT. RCT sẽ cung cấp khả năng liên lạc giữa một hoặc nhiều AE và một hoặc nhiều SPT và giám sát giao diện với một hoặc nhiều AE.

7.1.2 RCT có thể là một thành phần tích hợp của bất kỳ thiết bị tiếp nhận/thông báo nào hoặc là một thiết bị độc lập. Trong cả hai trường hợp, RCT phải đáp ứng các yêu cầu tại tiêu chuẩn này

7.2 Yêu cầu về cấp quyền truy cập logic (xem phụ lục C)

7.2.1 Truy cập vào tất cả các chức năng sẽ yêu cầu ủy quyền bằng khóa.

7.2.2 Mức truy cập 2, 3 và 4 sẽ sử dụng tài khoản cá nhân để đảm bảo khả năng truy xuất nguồn gốc (truy xuất các hành động đã thực hiện trong hệ thống). Người dùng mức độ 4 sẽ được người dùng có quyền truy cập mức độ 3 ủy quyền. Quyền này có thể là vĩnh viễn hoặc có giới hạn thời gian.

7.2.3 Truy cập ở mọi mức độ phải được ủy quyền bằng chìa khóa. Hệ thống tạo khóa phải có khả năng tạo ra ít nhất 1.000.000 khóa khác nhau.

7.2.4 Trong trường hợp nếu có hơn 3 lần truy cập không thành công trong khoảng thời gian 60 giây, RCT sẽ có khả năng trì hoãn các lần thử tiếp theo. Sau lần thử thứ ba, mỗi lần thử tiếp theo sẽ bị ngăn chặn trong tối thiểu 90 giây. Điều này phải được ghi lại trong RCT và phải gửi thông báo đến ATSP. Loại hành vi này phải được coi là hành vi cố ý tấn công hệ thống.

7.2.5 Nếu có khóa mặc định từ nhà sản xuất, hệ thống không được phép hoàn thành quá trình cài đặt RCT mà không thay đổi khóa mặc định đó trong quá trình cài đặt**.**

7.2.6 Truy cập từ xa phải yêu cầu kết nối an toàn và đáp ứng các yêu cầu bảo mật dữ liệu theo quy định tại Điều 5 và Điều 8 của tiêu chuẩn này.

7.2.7 Tự động đăng xuất khỏi các phiên truy cập từ xa sẽ được kích hoạt sau một thời gian không hoạt động. Khoảng thời gian này có thể cấu hình được để phù hợp yêu cầu bảo mật

7.2.8 Các quyền truy cập vào các chức năng theo các mức độ truy cập được nêu tại bảng 3

Bảng 3 - Mức truy cập - Truy cập logic vào các chức năng RCT

Mức truy cập	Mức 1	Mức 2	Mức 3	Mức độ 4
Xem các chỉ dẫn của RCT	Cho phép	Cho phép	Cho phép	Cho phép
Thay đổi cấu hình RCT	Không	Không	Cho phép	Không
Xem cấu hình RCT	Không	Cho phép	Cho phép	Cho phép
Cài đặt, kích hoạt, gỡ bỏ/tắt SPT	Không	Cho phép	Cho phép	Không
Xem Nhật ký sự kiện/báo động RCT	Không	Cho phép	Cho phép	Cho phép
Cập nhật/ thay đổi phần mềm RCT	Không	Không	Không	Cho phép
Thay đổi người dùng và/hoặc quyền của người dùng	Không	Không	Cho phép	Không
Thay đổi và/hoặc xóa các mục trong nhật ký sự kiện	Không	Không	Không	Không
Ghi chú: Yêu cầu “không” hoặc “cho phép” truy cập vào một chức năng nhất định không có nghĩa là bắt buộc phải thực hiện chức năng đó.				

7.3 Tải lên và tải xuống phần mềm

Việc tải lên và tải xuống phần mềm vào/ra khỏi RCT chỉ được phép ở mức truy cập phù hợp như quy định tại 7.2 và phụ lục C.

7.4 Lưu trữ các thông số và dữ liệu

Quá trình cấp nguồn lại (ví dụ sau khi mất điện và được khôi phục lại) hoặc khởi động lại phần mềm (ví dụ như cập nhật phần mềm, khắc phục lỗi…) sẽ không dẫn đến mất bất kỳ cấu hình, nhật ký và thông báo báo động đã được bảo vệ nào. RCT sẽ tự động trở lại hoạt động bình thường sau quá trình cấp nguồn hoặc khởi động lại phần mềm.

7.5 Giám sát và thông báo lỗi của ATP và ATS

RCT sẽ giám sát ATP và ATS. Các lỗi sẽ được báo cáo cho AMS theo quy định tại 5.3.3.4 của tiêu chuẩn này và được cung cấp cho ATSP. Tài liệu do nhà sản xuất cung cấp phải mô tả tín hiệu thông báo

7.6 Giao diện tới AMS

7.6.1 Các giao diện tới các AE phải được giám sát theo Điều 5 tiêu chuẩn này. Thời gian báo cáo lỗi kết nối phải nhỏ hơn hoặc bằng thời gian báo cáo của ATS hoặc 60 giây, tùy theo thời gian nào ngắn hơn. Trong trường hợp lỗi giao diện, thông báo lỗi sẽ được tạo ra và sự kiện sẽ được ghi lại.

7.6.2 Nhà sản xuất phải nêu trong tài liệu sản phẩm của họ các thông số kỹ thuật của giao diện tới I_{RcT} (AMS) và cách tín hiệu lỗi được trình bày và ghi lại.

7.6.3 Có thể cung cấp giao diện AE thay thế.

7.7 Tín hiệu lỗi

7.7.1 RCT phải có cơ chế để báo hiệu lỗi khi xảy ra bất kỳ lỗi nào sau đây:

a) Lỗi liên kết truyền dẫn giữa RCT (hoặc RCT-A đối với giải pháp lưu trữ) và AMS (Irc_T). Có thể không thể báo hiệu lỗi này tới AMS nếu đường truyền bị lỗi.

b) Trong trường hợp giải pháp lưu trữ, lỗi liên kết truyền dẫn giữa RCT-H và RCT- A;

c) Giao diện mạng truyền dẫn giữa RCT (hoặc RCT-H đối với giải pháp lưu trữ) và SPT (ví dụ vấn đề mã hóa);

d) Lỗi hệ thống RCT bên trong bao gồm cả sai lệch thời gian sau khi đưa vào vận hành.

7.7.2 Nhà sản xuất phải chỉ rõ trong tài liệu RCT cách các lỗi này được báo hiệu cho AMS, ATSP và cách thức kiểm tra cơ chế báo lỗi này.

7.8 Ghi lại sự kiện

7.8.1 RCT phải có chức năng ghi nhật ký nhằm mục đích truy vết và xử lý sự cố. Các sự kiện được ghi lại sẽ được quy định tại bảng 4.

7.8.2 Nhật ký sự kiện có thể được lưu trữ bên ngoài RCT.

7.8.3 Phương tiện ghi nhật ký phải sử dụng bộ nhớ không mất dữ liệu (non-volatile). Các dữ liệu trong

nhật ký phải được lưu giữ tối thiểu 3 năm. Nhà sản xuất phải nêu rõ trong tài liệu của họ cách thức thực hiện điều này.

7.8.4 Những sự kiện cũ hơn 3 năm có thể bị xóa.

7.8.5 Ngoài sự kiện, nhật ký phải ghi lại chính xác thời gian và ngày tháng mà sự kiện xảy ra. Độ phân giải thời gian tối thiểu phải là 1 giây và phải chính xác theo giờ chuẩn quốc tế (UTC) trong phạm vi ± 5 giây.

7.8.6 RCT sẽ cung cấp phương tiện để đồng bộ hóa ngày và giờ UTC. Nhà sản xuất sẽ chỉ rõ trong tài liệu của họ cách đồng bộ hóa thời gian với UTC.

7.8.7 RCT có thể sử dụng múi giờ địa phương.

7.8.8 Để tối ưu hóa việc lưu trữ các sự kiện, nếu các sự kiện giống hệt nhau xảy ra trong bất kỳ khoảng thời gian 12 giờ nào, thì chỉ cần ghi lại sự kiện đầu tiên và sự kiện cuối cùng. Khi thực hiện cách này thì phải ghi lại số lượng các sự kiện giống hệt nhau**.**

7.8.9 Đối với các mục có yêu cầu bắt buộc nhận dạng người dùng tại Bảng 4, việc ghi nhật ký truy cập vào RCT phải bao gồm cả việc nhận dạng người dùng**.**

Bảng 4 - Sự kiện cần ghi của RCT

STT	Sự kiện cần ghi	Nhận dạng người dùng
1	Thông báo báo động và cảnh báo từ ATS	Không bắt buộc
2	Giao diện AE bị lỗi và khôi phục	Không bắt buộc
3	Các giao diện mạng truyền dẫn bị lỗi và khôi phục	Không bắt buộc
4	Thay đổi cấu hình của RCT	Bắt buộc
5	Bật nguồn hoặc thiết lập lại (reset)	Bắt buộc
6	Bất kỳ thay đổi nào đối với phần mềm	Bắt buộc
7	Thay đổi ngày và giờ	Bắt buộc
8	Truy cập vào RCT	Bắt buộc
9	Thay đổi đối với người dùng và/hoặc quyền của người dùng	Bắt buộc
GHI CHÚ Việc ghi lại thông tin nhận dạng người dùng chỉ bắt buộc nếu sự kiện được kích hoạt bởi sự can thiệp của người dùng.		

7.9 Chế độ vận hành (lưu và chuyển tiếp hoặc truyền thẳng)

7.9.1 Tổng quan

7.9.1.1 Có hai chế độ hoạt động được phép:

a) Lưu và chuyển tiếp;

b) Truyền thẳng

7.9.1.2 Nhà sản xuất sẽ tuyên bố trong tài liệu sản phẩm của mình những chế độ vận hành nào được hỗ trợ.

7.9.2 Yêu cầu đối với chế độ vận hành lưu và chuyển tiếp

7.9.2.1 Khi nhận được thông báo cảnh báo, báo động từ SPT, RCT sẽ bảo đảm an toàn cho các tin nhắn báo động và gửi xác nhận đã nhận được báo động chính xác cho SPT.

7.9.2.2 Nếu sử dụng chế độ lưu và chuyển tiếp, tất cả các thông báo cảnh báo, báo động phải bao gồm dấu thời gian ngày và giờ khi SPT nhận được thông báo.

7.9.2.3 RCT cũng có thể ghi lại ngày và giờ khi thông báo cảnh báo, báo động được chuyển tiếp đến AE và/hoặc khi nhận được xác nhận từ AE.

7.9.2.4 Việc bảo vệ thông báo cảnh báo, báo động sẽ được thực hiện bằng cách lưu trữ thông báo trong bộ nhớ không mất dữ liệu (non-volatile) của RCT, điều này nhằm bảo vệ các thông báo đã xác nhận khi giao diện AE bị lỗi hoặc trong thời gian mất điện. Các thông báo đã lưu trữ sẽ được truyền đi khi tình trạng lỗi được xóa.

7.9.2.5 Thông báo cảnh báo, báo động được bảo vệ sẽ được truyền từ RCT đến các AE.

7.9.2.6 Việc tiếp nhận, xác nhận từ các AE sẽ không được chuyển tiếp đến SPT, vì SPT đã nhận được xác nhận từ RCT.

Ghi chú: Việc mất thông báo cảnh báo, báo động được coi là tình huống tệ hơn so với việc gửi thông báo bị chậm trễ.

7.9.3 Yêu cầu hoạt động truyền thẳng

7.9.3.1 Khi nhận được thông báo cảnh báo, báo động từ SPT, RCT sẽ phải chuyển tiếp thông báo đến các AE.

7.9.3.2 RCT sẽ không được xác nhận thông báo cảnh báo, báo động cho SPT trước khi nhận được xác nhận từ ít nhất một AE. Khi RCT nhận được xác nhận từ AE, xác nhận sẽ được chuyển tiếp đến SPT.

7.10 Từ chối dịch vụ

Nhà sản xuất RCT cung cấp phương pháp được sử dụng để đảm bảo quy định tại 5.2.5.

7.11 Bảo mật thông tin

Nhà sản xuất phải cung cấp phương pháp được sử dụng để đảm bảo quy định tại 5.8.3 áp dụng cho cả giao tiếp của SPT và truy cập từ xa

7.12 Bảo mật chống giả mạo

Nhà sản xuất phải cung cấp phương pháp được sử dụng để đảm bảo quy định tại 5.8.2.

7.13 RCT dự phòng

Nhà sản xuất phải chỉ rõ và chứng minh đảm bảo dự phòng RCT theo quy đinh tại 5.1.2

7.14 Tài liệu

7.14.1 Tài liệu liên quan đến RCT phải ngắn gọn, đầy đủ và rõ ràng. Thông tin phải được cung cấp đủ để lắp đặt, đưa vào vận hành, vận hành và bảo trì RCT.

7.14.2 Các hướng dẫn liên quan đến hoạt động của RCT phải được thiết kế để giảm thiểu khả năng hoạt động không chính xác và được cấu trúc để phản ánh mức truy cập của người dùng.

7.14.3 Trong trường hợp có các bộ phận mà người dùng có thể tự bảo dưỡng (ví dụ cầu chì), loại và giá trị của chúng sẽ được cung cấp.

7.14.4 Tài liệu phải bao gồm:

a) Tên nhà sản xuất hoặc nhà cung cấp,

b) Mô tả thiết bị,

c) Tiêu chuẩn áp dụng,

d) Nhãn hiệu hoặc dấu hiệu của tổ chức chứng nhận,

đ) Số lượng SPT tối đa có thể kết nối,

e) Số lượng AE tối đa có thể kết nối,

f) Số lượng tối đa các giao diện mạng truyền dẫn,

g) Số lượng cảnh báo, báo động tối đa có thể xử lý được mỗi giây,

h) Danh sách các danh mục ATS được hỗ trợ,

i) Yêu cầu về nguồn điện.

7.15 Ghi nhãn

7.15.1 RCT phải được ghi nhãn thể hiện các nội dung như sau:

- Tên hoặc dấu hiệu của nhà sản xuất;

- Chủng loại ATS phù hợp với RCT.

7.15.2 Việc ghi nhãn phải dễ đọc, bền vững và không gây nhầm lẫn. Nếu RCT không sử dụng phần cứng chuyên dụng (ví dụ RCT là giải pháp phần mềm), phần mềm phải có khả năng hiển thị các nội dung ghi nhãn quy định tại 7.15.1.

8 Yêu cầu đối với truy cập từ xa

8.1 Yêu cầu chung

8.1.1 Hạ tầng truy cập từ xa (RAI) bao gồm 3 chức năng: RAE, RAS và RAC.

8.1.2 RAI phải được thiết kế sao cho chỉ cho phép các kết nối giữa RAE và RAS ở một đầu, và các kết nối giữa RAS và RAC ở đầu kia. Kết nối giữa RAC và RAE chỉ có thể thực hiện thông qua RAS. Không được phép thiết lập kết nối trực tiếp giữa RAC và RAE**.**

8.1.3 RAI được chia sẻ với các ứng dụng khác phải được sắp xếp sao cho việc vận hành và bảo trì không ngăn cản RAI đáp ứng các yêu cầu của Điều 8 tiêu chuẩn này

8.2 Yêu cầu đối với bảo mật thông tin

8.2.1 Yêu cầu chung

8.2.1.1 Tất cả thông tin được lưu trữ và truyền tải trong RAI phải được bảo mật.

8.2.1.2 Nhà cung cấp dịch vụ hạ tầng truy cập từ xa (RAISP) phải áp dụng các biện pháp bảo mật để bảo vệ RAI và các thành phần của nó khỏi các cuộc tấn công độc hại và các tác động không mong muốn. RAISP phải mô tả các biện pháp bảo mật này trong tài liệu kỹ thuật.

Ghi chú: Những thông tin mà RAISP coi là bí mật không cần phải công khai trong tài liệu kỹ thuật.

8.2.1.3 Tất cả các yêu cầu về bảo mật thông tin được áp dụng cho việc giao tiếp giữa RAE và RAS, cũng như giữa RAS và RAC

8.2.1.4 RAISP có thể ủy thác một số trách nhiệm thông qua các hợp đồng với ATSP (Nhà cung cấp dịch vụ truyền tín hiệu báo động), MARC (Trung tâm giám sát và tiếp nhận báo động), nhà điều hành mạng truyền tải, v.v., nhưng vẫn phải chịu trách nhiệm tổng thể.

8.2.2 Tính toàn vẹn và bảo mật dữ liệu

8.2.2.1 Tính toàn vẹn dữ liệu phải được đảm bảo cho tất cả các phiên làm việc bằng cách sử dụng kỹ thuật hàm băm (hasing) hoặc chữ ký số đáp ứng các yêu cầu tại 5.8.1

8.2.2.2 Tất cả các phiên làm việc phải được mã hóa để đảm bảo tính bảo mật. Các yêu cầu về mã hóa tương tự như tại 5.8.1

8.2.3 Xác thực

8.2.3.1 Xác thực kết nối

Các biện pháp phải được cung cấp để xác thực RAE, RAS và RAC. RAS chỉ cho phép các kết nối từ RAE và RAC đã được xác thực. RAISP phải chỉ rõ cách thức xác thực được thực hiện và cách thức quản lý các chức năng đã được xác thực.

8.2.3.2 Xác thực phiên làm việc cho người dùng từ xa

8.2.3.2.1 Các biện pháp phải được cung cấp để hạn chế truy cập từ xa vào RAS bằng cách chỉ cho các tài khoản người dùng từ xa đã được xác thực và xác nhận duy nhất, yêu cầu người dùng từ xa cung cấp ít nhất hai trong các yếu tố nhận dạng sau:

a) Những gì người dùng từ xa có: Yếu tố dựa trên phần mềm hoặc phần cứng (ví dụ: Chứng thư số (token), thẻ thông minh hoặc ứng dụng bảo mật tạo mật khẩu một lần (OTP) dựa trên thời gian).

b) Những gì người dùng từ xa biết: (ví dụ: mật khẩu, mã PIN, câu hỏi bảo mật).

c) Những gì thuộc về xác thực sinh trắc học của người dùng từ xa là: (ví dụ: vân tay, nhận diện khuôn mặt, mống mắt).

8.2.3.2.2 Người dùng từ xa sử dụng RAC để truy cập từ xa phải luôn sử dụng xác thực hai yếu tố.

8.2.3.2.3 RAISP phải có một chính sách thông tin xác thực được lập thành tài liệu.

8.2.3.2.4 RAS phải từ chối tất cả các nỗ lực phiên làm việc từ người dùng chưa được xác thực.

8.2.3.2.5 Tất cả thông tin người dùng từ xa trong RAI phải được bảo vệ chống lại việc truy cập trái phép.

8.2.3.2.6 RAISP phải xác định số lần thử đăng nhập trong một khoảng thời gian nhất định để hạn chế rủi ro tấn công dò tìm mật khẩu (brute force attack).

8.2.3.2.7 Nếu người dùng không hoạt động sau một khoảng thời gian nhất định, phiên làm việc sẽ hết hạn. Để tiếp tục truy cập, người dùng cần xác thực lại. Việc yêu cầu xác thực lại này có thể cấu hình. Các giá trị thích hợp cho thời gian hết hạn phụ thuộc vào từng trường hợp sử dụng và phải được RAISP xác định

8.2.4 Ủy quyền

8.2.4.1 RAISP phải cung cấp phương pháp để quản lý quyền truy cập vào RAI cho người dùng từ xa và/hoặc các hệ thống bên thứ ba trước khi cho phép truy cập ATS. Cách thức phân quyền được thực hiện phải thể hiện trong tài liệu của RAISP.

8.2.4.2 Giao diện bên ngoài cho hệ thống bên thứ ba

8.2.4.2.1 Khi RAI cung cấp một giao diện bên ngoài để cho phép các hệ thống bên thứ ba truy cập vào RAI, RAC phải đảm bảo rằng quá trình phân quyền được thực hiện.

8.2.4.2.2 RAISP phải xác định cách RAC đảm bảo rằng một hệ thống bên thứ ba kết nối với RAI là đáng tin cậy.

Ví dụ: Một ví dụ về phương pháp giao diện bên ngoài có thể là một API (Giao diện lập trình ứng dụng) bảo mật, cho phép giao tiếp giữa các ứng dụng.

Ghi chú 1: Khi sử dụng API, có thể áp dụng OAuth2.0 hoặc các phương thức tương đương để thực hiện phân quyền.

Ghi chú 2: RAISP không chịu trách nhiệm đối với các hệ thống bên thứ ba, nhưng RAISP chịu trách nhiệm đảm bảo rằng quá trình phân quyền được thực hiện thành công

8.2.5 Ghi nhật ký

8.2.5.1 Để quản lý và theo dõi, RAISP phải thực hiện việc giám sát và ghi nhật ký ít nhất các sự kiện sau:

a) Đăng nhập và đăng xuất của người dùng đã xác thực;

b) Kết nối đã xác thực từ RAE tới RAS;

c) Kết nối đã xác thực từ RAC tới RAS;

d) Các thay đổi cấu hình RAI do RAISP thực hiện;

e) Các thay đổi thông tin tài khoản và quyền hạn;

f) Các sự kiện liên quan đến bảo mật.

Ghi chú: Các sự kiện liên quan đến bảo mật là các sự kiện mà trong đó bảo mật của RAI đã bị xâm phạm hoặc có dấu hiệu cố gắng xâm phạm bảo mật đã được phát hiện.

8.2.5.2 Tất cả các mục ghi nhật ký đã liệt kê phải được ghi lại ít nhất trên RAS và có dấu thời gian ngày, giờ theo chuẩn UTC.

8.2.5.3 Tất cả các mục ghi nhật ký đã liệt kê phải có độ chính xác trong vòng 3 giây so với múi giờ UTC.

8.2.5.4 Tất cả các bản ghi nhật ký phải được lưu trữ trong ít nhất 1 năm.

8.2.5.5 RAISP phải có các quy trình để xem xét định kỳ nhật ký và thực hiện các biện pháp khắc phục nếu cần thiết.

8.3 Yêu cầu về hiệu suất

Các tiêu chí và mức độ hiệu suất phải được thỏa thuận và ghi chép giữa các bên. RAISP phải có quy trình để giám sát và quản lý hiệu suất đã thỏa thuận.

Ghi chú: Các tiêu chí và mức độ hiệu suất là các yêu cầu cụ thể về hiệu suất của hệ thống, chẳng hạn như tốc độ truy cập, độ trễ, khả năng chịu tải, và các yêu cầu về tính sẵn sàng

8.4 Yêu cầu về chức năng

8.4.1 Khách hàng Truy cập Từ xa (RAC)

8.4.1.1 Trong RAI, RAC là phần chức năng cần thiết để thiết lập kết nối đáng tin cậy và an toàn với RAS. Vì RAC như được định nghĩa trong tài liệu này không phải là một thiết bị vật lý, các phần chức năng sẽ cần được triển khai trên một số thiết bị nào đó. Tiêu chuẩn này không quy định yêu cầu vật lý cho các thiết bị như vậy.

8.4.1.2 RAISP chịu trách nhiệm quản lý các RAC.

8.4.1.3 Khi RAC được triển khai trên thiết bị người dùng, RAISP không chịu trách nhiệm về phần cứng của thiết bị đó.

8.4.1.4 Chức năng RAC có thể là một phần tích hợp của ứng dụng trên máy tính để bàn và/hoặc ứng dụng di động.

8.4.1.5 RAISP được khuyến nghị cung cấp hướng dẫn cho chủ sở hữu của thiết bị lưu trữ RAC về cách thực hiện các biện pháp an ninh mạng phù hợp.

8.4.2 Máy chủ truy cập từ xa (Remote Access Server)

8.4.2.1 RAS là chức năng trung tâm của hạ tầng truy cập từ xa. RAS phải quản lý các kết nối an toàn giữa một hoặc nhiều RAE và một hoặc nhiều RAC. RAS cũng phải quản lý việc xác thực và phân quyền cho người dùng từ xa và các hệ thống bên thứ ba.

8.4.2.2 Nếu RAS là một chức năng tích hợp của thiết bị hoặc hệ thống khác thì vẫn phải đáp ứng quy định tại Điều 8 của tiêu chuẩn này.

8.4.2.3 RAS phải được lưu trữ tại một vị trí an toàn. RAISP chịu trách nhiệm quản lý RAS

Ghi chú 1: Không có yêu cầu về phần cứng lưu trữ phần mềm của RAS.

Ghi chú 2: Để bảo đảm an toàn và hiệu suất hệ thống, chỉ sử dụng một RAI để tiếp nhận thông tin từ FDAD qua ATS.

8.4.3 Điểm cuối Truy cập Từ xa (RAE)

8.4.3.1 RAE là điểm cuối chức năng của hạ tầng truy cập từ xa và chịu trách nhiệm giao tiếp với ATS và quản lý kết nối an toàn với RAS.

8.4.3.2 Nếu RAE là một chức năng tích hợp của một thiết bị hoặc hệ thống khác, các yêu cầu của tài liệu này vẫn áp dụng.

8.4.3.3 RAE không được ảnh hưởng xấu đến hoạt động và/hoặc hiệu suất của hệ thống cảnh báo kết nối.

8.4.3.4 RAE phải được lưu trữ tại các cơ sở được giám sát

Ghi chú: Không có yêu cầu về phần cứng lưu trữ RAE.

8.4.3.5 Chức năng RAE có thể được tích hợp vào SPT, RCT hoặc bất kỳ thiết bị nào khác.

8.4.4 Tài liệu

RAISP phải duy trì tài liệu đầy đủ để phục vụ cho việc lập kế hoạch, cài đặt, đưa vào vận hành, bảo trì và hoạt động của RAI.

8.5 Yêu cầu vận hành

8.5.1 RAISP phải có một hệ thống quản lý an ninh thông tin hoặc các tiêu chuẩn báo cáo được thiết lập và cập nhật thường xuyên**.**

Ghi chú: ISO/IEC 27001 là một ví dụ về tiêu chuẩn hệ thống quản lý an ninh thông tin.

8.5.2 Tối thiểu, RAISP phải có các quy trình quản lý rủi ro vận hành được ghi chép đầy đủ và sau đây:

a) Quy trình quản lý rủi ro liên quan đến Công nghệ (Technology).

b) Quy trình quản lý rủi ro liên quan đến Quản lý Liên tục (Continuity Management).

c) Quy trình quản lý rủi ro liên quan đến Quản lý Rủi ro (Risk Management).

d) Quy trình quản lý rủi ro liên quan đến Quản lý Danh tính (Identity Management).

đ) Quy trình quản lý rủi ro liên quan đến Quản lý Cấu hình (Configuration Management).

e) Quy trình quản lý rủi ro liên quan đến An ninh mạng (Cybersecurity).

9 Kiểm tra, thử nghiệm

9.1 Kiểm tra hiệu suất ATS

9.1.1 Quy định chung

9.1.1.1 Việc kiểm tra hiệu suất của ATS được thực hiện để đảm bảo việc giám sát tất cả các bộ phận của ATS có hiệu quả và các tín hiệu lỗi được tạo ra và truyền thành công trong trường hợp phát hiện lỗi ATS

9.1.1.2 Việc kiểm tra hiệu suất của ATS sẽ bao gồm:

a) Kiểm tra để xác minh rằng hoạt động cơ bản của hệ thống tuân thủ các yêu cầu của Điều 5 tiêu chuẩn này và các tiêu chuẩn hiện hành có liên quan, bao gồm việc thử nghiệm để xác nhận rằng các báo động được truyền đi và ATS được giám sát;

b) Kiểm tra thường xuyên hoặc định kỳ để xác nhận tính khả dụng của ATS

Ghi chú: Việc thử nghiệm giao diện SPT và FDAD được thực hiện theo 9.2 của tiêu chuẩn này

9.1.2 Hiệu suất ATSN

9.1.2.1 Khi các FDAD tạo thành một số nhóm riêng biệt về mặt địa lý và khi các nhóm này giao tiếp với các máy thu riêng biệt trong trung tâm tiếp nhận hoặc có thể được xác định riêng biệt theo cách khác thì mỗi nhóm có thể được xem là một ATSN riêng biệt. Khi sử dụng phép chia này, việc kiểm tra sẽ được thực hiện riêng biệt trên từng nhóm đã xác định. ATSP sẽ thống nhất các tiêu chí được sử dụng phân chia ATS thành các ATSN.

9.1.2.2 Việc xác minh hiệu suất của ATSN sẽ đảm bảo rằng, đối với cấu hình hệ thống và số lượng FDAD được kết nối dự kiến, ATSN có khả năng đáp ứng các yêu cầu của 5.2. Điều này sẽ được thực hiện bằng cách xác minh hiệu suất của các ATS đã được đưa vào vận hành đầy đủ.

9.1.3 Thời gian truyền

9.1.3.1 Việc truyền báo động chính xác phải được kiểm tra, bao gồm cả việc truyền cảnh báo liên quan đến giám sát ATS. Thời gian truyền, ví dụ như báo động thử nghiệm FDAD, phải đáp ứng quy định tại 5.3.2

9.1.3.2 Thời gian báo cáo (phát hiện và truyền tín hiệu lỗi) do lỗi của ATP từ FDAD tại cơ sở được giám sát đến AE tại ARC phải đáp ứng yêu cầu tại Bảng 1.

9.1.4 Tần suất kiểm tra hiệu suất

9.1.4.1 Việc kiểm tra hiệu suất theo quy định tại 5.3 và Bảng 1 của ATS phải được thực hiện thường xuyên và trong các trường hợp sau:

a) lần đầu đưa ATS vào vận hành;

b) sau bất kỳ thay đổi nào của ATS (thay đổi ATE và/hoặc mạng truyền dẫn).

9.1.4.2 Trong trường hợp tốc độ truyền báo động qua hệ thống thay đổi theo thời gian hoặc trong trường hợp việc sử dụng ATS của các dịch vụ khác sử dụng cùng một thiết bị thay đổi theo thời gian (ví dụ như hệ thống sử dụng mạng điện thoại công cộng hoặc PSN dùng chung), thì việc phân bổ thời gian thực hiện xác minh hiệu suất phải phản ánh sự phân bổ thời gian trong ngày hoặc tuần mà các thông báo thực tế dự kiến sẽ xảy ra.

9.1.4.3 Kết quả kiểm tra của từng ATS và ATSN phải được phân tích qua các giai đoạn liên tiếp kéo dài 3 tháng. Tuy nhiên, điều này không có nghĩa là từng ATS và ATSN phải được kích hoạt và kiểm tra trong mọi giai đoạn 3 tháng đó.

9.1.5 Tính khả dụng

9.1.5.1 Hồ sơ

9.1.5.1.1 Tất cả các lỗi và các lần kiểm tra hiệu suất trên mọi ATS và mạng ATSN phải được ghi nhận và lưu trữ bởi ATSP.

9.1.5.1.2 Các lỗi liên quan đến đường truyền hoặc thiết bị dự phòng cũng cần được ghi lại nếu chúng ảnh hưởng đến yêu cầu về tính khả dụng được quy định tại tiêu chuẩn này.

9.1.5.1.3 Thông tin cần lưu trữ cho mỗi lỗi của ATS bao gồm:

a) thời gian và ngày xác định lỗi,

b) thời gian và ngày hệ thống được khắc phục và khôi phục hoạt động bình thường..

9.1.5.1.4 Hồ sơ phải được lưu giữ trong thời gian không dưới ba năm.

9.1.5.1.5 Hồ sơ về tính khả dụng của ATS và ATSN phải được cung cấp cho khách hàng khi được yêu cầu.

9.1.5.1.6 Các hồ sơ sẽ được ATSP cung cấp cho các bên quan tâm (ví dụ: ARC, đơn vị lắp đặt, người dùng cuối, cơ quan chứng nhận, cơ quan quản lý).

9.1.5.1.7 Có thể truy vết các lỗi của ATP và ATS riêng lẻ trong dữ liệu tóm tắt để phân tích lỗi và thời điểm thực hiện hành động khắc phục.

9.1.5.2 Tính toán

9.1.5.2.1 Tổng quan

Các hồ sơ ghi nhận về tất cả các lần kiểm tra hiệu suất được thực hiện trên ATS và/hoặc ATSN sẽ được sử dụng để xác định tính khả dụng của ATS và ATSN.

9.1.5.2.2 Tính toán tính khả dụng của ATS

Khi mỗi lần một ATS không khả dụng (xem 5.7.3), thời gian lỗi của mỗi lỗi đơn lẻ sẽ được xác định. Đối với mỗi khoảng thời gian bảy ngày, tính khả dụng của ATS sẽ được tính như sau:

$$WA = (1 - \frac{WF}{10080})\text{x}100\%$$

Trong đó:

WA: Tính khả dụng tính theo tuần, biểu thị theo phần trăm:

WF: Tổng thời gian lỗi trong khoảng thời gian bảy ngày, tính theo phút như quy định tại 5.7.4

Ghi chú: 10 080 = 7 ngày x 24 giờ x 60 phút, là số phút trong một tuần.

9.1.5.2.3 Tính toán khả dụng của ATSN

a) Xác định thời gian lỗi của ATSN theo công thức:

FT=DFxNA

Trong đó:

FT: Thời gian lỗi của ATSN, được biểu thị bằng phút;

DF: Thời gian lỗi của mỗi lỗi, tính theo phút như quy định tại 5.7.4

NA: số FDAD bị ảnh hưởng bởi lỗi

b) Xác đinh tổng thời gian lỗi hàng năm của ASTN theo công thức:

$$YF = \sum_{i=1}^{n} FTi$$

Trong đó:

FTi: Các thời gian lỗi của của mỗi lỗi ASTN

c) Xác định tính khả dụng của ATSN theo công thức

$$YA = \left(1 - \frac{YF}{525\,600 \times NC}\right) \times 100\,\%$$

Trong đó:

YA: Tính khả dụng trong một năm của ASTN, biểu thị theo phần trăm.

YF: Tổng thời gian lỗi hàng năm của ASTN, được thể hiện bằng phút.

NC: tổng số FDAD được kết nối.

Ghi chú: 525 600 = 365 ngày x 24 giờ x 60 phút, là số phút trong một năm

9.1.5.2.4 Tổng thời gian lỗi phải bao gồm tất cả các lỗi, kể cả lỗi đã được khắc phục trong năm. Số lượng ATS sử dụng để tính toán tính khả dụng của ASTN sẽ là số lượng ATS tính từ thời điểm 00h:00 của ngày cuối cùng của năm. Tính khả dụng của hệ thống hàng năm sẽ là trung bình số học của tính khả dụng hàng tuần trong 52 tuần liên tiếp.

Ví dụ: Giả sử chu kỳ tính toán bắt đầu từ ngày 1 tháng 1 năm 2025 và kết thúc vào ngày 31 tháng 12 năm 2025, thì số lượng ATS sẽ được ghi nhận vào cuối ngày 31 tháng 12 khi chuyển sang ngày 1 tháng 1 năm 2026 00h:00 ngày 01/01/2026. Vào thời điểm này, sẽ tính đến tất cả các ATS đã được triển khai trong năm (2026) và sử dụng số lượng đó để tính toán mức độ sẵn sàng của hệ thống trong chu kỳ năm 2026

9.1.5.2.5 Khi hệ thống thay đổi quy mô thì tính khả dụng của quy mô hệ thống mới không cần phải thay đổi chu kỳ bảy ngày liên tục.

Ghi chú: Khi hệ thống tăng hoặc giảm ATS, thì tính mức khả dụng chu kỳ 7 ngày của hệ thống vẫn được tiếp tục tính, không cần bắt đầu xác định lại chu kỳ 7 ngày mới.

9.1.5.2.6 Kết quả và tính toán phải được lưu giữ trong thời gian không dưới ba năm.

9.2 Kiểm tra, thử nghiệm SPT

9.2.1 Yêu cầu chung

9.2.1.1 Các điều kiện môi trường không khí cho thử nghiệm

Nếu không có quy định nào khác trong một quy trình thử cụ thể (ví dụ như các thử nghiệm môi trường), thì phép thử phải được thực hiện sau khi mẫu thử đã được để ổn định trong các điều kiện môi trường tiêu chuẩn dành cho thử nghiệm theo như mô tả trong TCVN 7699-1 (IEC 60068-1), cụ thể như sau:

- Nhiệt độ: 15 °C đến 35 °C;

- Độ ẩm tương đối: 25 % đến 75 %;

- Áp suất không khí: 86 kPa đến 106 kPa

Nếu các sai lệch về những thông số có ảnh hưởng đến kết quả đo, thì những sai lệch đó phải được giữ ở mức tối thiểu trong suốt quá trình thực hiện các phép đo là một phần của một thử nghiệm trên một mẫu.

9.2.1.2 Chuẩn bị mẫu thử

9.2.1.2.1 Cấu hình của mẫu thử

a) Cấu hình của mẫu thử ít nhất phải bao gồm tất cả các dạng SPT và đường truyền dẫn. Báo cáo thử nghiệm phải cung cấp các chi tiết của SPT.

b) Các thành phần ATS khác như FDAD, mạng và RCT có thể được cung cấp dưới dạng thiết bị mô phỏng và/hoặc mạng mô phỏng. Khi cần RCT (hoặc RCT mô phỏng) cho các bài kiểm tra, RCT đó phải có khả năng đáp ứng các yêu cầu của Điều 8 tiêu chuẩn này.

c) Trong các thử nghiệm, thiết bị khác không phải là SPT có thể được đặt trong điều kiện môi trường không khí tiêu chuẩn

d) Việc lắp đặt, cấu hình mẫu thử phải theo hướng dẫn của nhà sản xuất.

9.2.1.2.2 Bố trí lắp đặt

Mẫu thử nghiệm phải được lắp đặt ở phương hướng bình thường bằng các chi tiết gắn kết thông thường phù hợp với hướng dẫn của nhà sản xuất. Thiết bị phải được đặt ở điều kiện mức truy cập 1, ngoại trừ khi có yêu cầu đối với thử nghiệm về chức năng.

9.2.1.2.3 Đấu nối điện

a) Nếu quy trình thử nghiệm yêu cầu mẫu thử phải ở trạng thái vận hành, thì nó phải được nối với một nguồn cấp điện phù hợp với các yêu cầu trong TCVN 7568-4 (ISO 7240-4).

b) Trừ khi có yêu cầu khác, nguồn cấp điện phải phải ở trạng thái vận hành danh định.

c) Mọi mạch dẫn và đường truyền dẫn phải được nối với dây và thiết bị hoặc các phụ tải bù. Ít nhất phải có một mẫu mạch của mỗi một loại mạch dẫn phải chịu tác động của phụ tài lớn nhất, tất cả phải nằm trong quy định của nhà sản xuất.

9.2.2 Chương trình thử nghiệm và số lượng mẫu thử.

9.2.2.1 Chương trình thử nghiệm bao gồm các thử nghiệm chức năng ở điều kiện môi trường quy định tại 9.2.1.1, trong hoặc kế tiếp thử nghiệm chức năng là các thử nghiệm môi trường. Sau mỗi thử nghiệm môi trường, mẫu sẽ phải tiếp tục kiểm tra lại bằng các thử nghiệm chức năng.

Ghi chú: Đối với mỗi mẫu, thử nghiệm chức năng sau một thử nghiệm môi trường có thể được coi là thử nghiệm chức năng trước thử nghiệm môi trường tiếp theo (xem 9.2.2.4)

9.2.2.2 Thử nghiệm chức năng

Các chương trình thử nghiệm chức năng của SPT được tóm tắt tại bảng 5, quy định tại Phụ lục D

Bàng 5 – Tóm tắt các bài thử nghiệm chức năng của SPT

Điều, khoản	Yêu cầu kiểm tra	Mục tiêu kiểm tra/đánh giá	Phương pháp
6.1.1, 6.1.2, 6.1.3, 6.1.7, 6.2.6	Hoạt động của SPT	Chứng minh khả năng của SPT trong việc tiếp nhận, chuyển tiếp tín hiệu báo động, chỉ báo trạng thái và tạo ra các thông báo cảnh báo	Kiểm tra (mục 1.1 phụ lục D)
6.1.4	Báo cáo lỗi ATS cho FDAD	Khả năng của SPT trong việc báo cáo lỗi ATS cho FDAD	Kiểm tra (mục 1.2 phụ lục D)
6.1.5 và phụ lục G	Giao diện tới FDAD (nối tiếp)	Để chứng minh rằng bất kỳ giao diện nào có sẵn đều phải tuân thủ tài liệu của nhà sản xuất SPT	Xác thực (mục 1.3.1 phụ lục D)
	Giao diện tới FDAD (song song)	Để chứng minh rằng giao diện SPT phải tuân thủ Phụ lục G	Kiểm tra (mục 1.3.2 phụ lục D)
	Giao diện tới FDAD (độc quyền)	Để chứng minh rằng bất kỳ giao diện nào có sẵn đều phải tuân thủ tài liệu của nhà sản xuất SPT	Xác thực (mục 1.3.3 phụ lục D)
6.1.6	Giám sát giao diện mạng truyền dẫn	chứng minh rằng SPT có thể phát hiện lỗi ATP khi mỗi giao diện mạng truyền dẫn bị lỗi	Kiểm tra (mục 1.4 phụ lục D)
6.1.8 và phụ lục C	Mức độ truy cập	Chứng minh rằng tất cả các mức truy cập đều tồn tại	Kiểm tra (mục 1.5 phụ lục D)
6.1.9	Bảo mật chống giả mạo	Xác minh tuyên bố của nhà sản xuất về cách thức Bảo mật chống giả mạo được thực hiện và tuân thủ các yêu cầu của 6.3.5	Xác thực (mục 1.6 phụ lục D)

Điều, khoản	Yêu cầu kiểm tra	Mục tiêu kiểm tra/đánh giá	Phương pháp
6.1.10	Bảo mật thông tin	Xác minh tuyên bố của nhà sản xuất về cách thức bảo mật thông tin được triển khai và tuân thủ các yêu cầu của 6.3.6	
6.1.12	Tải lên và tải xuống phần mềm và chương trình cơ sở	Chứng minh rằng SPT sẽ phục hồi sau khi tải lên/tải xuống phần mềm và chương trình cơ sở không thành công	Kiểm tra (mục 1.7 phụ lục D)
6.1.13	Lưu trữ thông số	Chứng minh rằng việc lưu trữ của SPT không bị ảnh hưởng bởi mất điện	Kiểm tra (mục 1.8 phụ lục D)
6.1.14	Bảo vệ nhật ký	Để chứng minh sự tuân thủ theo tài liệu của nhà sản xuất	Xác thực (mục 1.10 phụ lục D)
	Khả năng lưu trữ và độ bền nhật ký	Để chứng minh khả năng lưu trữ số lượng sự kiện	Kiểm tra (mục 1.11 phụ lục D)
	Độ phân giải thời gian	Để chứng minh dấu thời gian kèm theo sự kiên	Kiểm tra (mục 1.12 phụ lục D)
	Ghi nhật ký sự kiện	Để chứng minh sự tuân thủ với Bảng 2	Kiểm tra (mục 1.9 phụ lục D)
6.2.2	Tài liệu	Kiểm tra tài liệu của nhà sản xuất theo yêu cầu của 6.4.2	Xác thực (mục 1.13 phụ lục D)
6.2.2	Phương pháp xác định hiệu suất ATS	Xác minh tuyên bố của nhà sản xuất về cách thức xác minh hiệu suất được thực hiện và tuân thủ các yêu cầu của 6.4.2	Xác thực (mục 1.14 phụ lục D)
Kiểm tra: Là các bài kiểm tra thử nghiệm vận hành thực tế để chứng minh rằng thiết bị đáp ứng yêu cầu; Xác thực: Là việc kiểm tra tài liệu của nhà sản xuất để đảm bảo việc đáp ứng các yêu cầu.			

9.2.2.3 Thử nghiệm môi trường

9.2.2.3.1 Phải thực hiện một thử nghiệm chức năng trước, trong và/hoặc sau mỗi thử nghiệm môi trường để đánh giá hoạt động của SPT.

9.2.2.3.2 Các chương trình thử nghiệm môi trường của SPT được tóm tắt tại bảng 6, quy định tại Phụ lục D

Bảng 6. Tóm tắt các bài thử nghiệm môi trường của SPT

Phép thử	Vận hành hoặc độ bền	Điều khoản
Điều kiện lạnh	Vận hành	2.1 Phụ lục D
Điều kiện ẩm nhiệt, trạng thái ổn định	Vận hành	2.2 Phụ lục D
Va đập	Vận hành	2.3 Phụ lục D
Rung, dao động sin	Vận hành	2.4 Phụ lục D
Tính tương thích điện tử (EMC), thử kháng nhiễm	Vận hành	2.5 Phụ lục D
Sự biến đổi của điện thế nguồn cấp	Vận hành	2.6 Phụ lục D
Điều kiện ẩm nhiệt, trạng thái ổn định	Độ bền	2.7 Phụ lục D
Rung, dao động sin	Độ bền	2.8 Phụ lục D

9.2.2.4 Số lượng mẫu thử.

9.2.2.4.1 Ít nhất phải cung cấp 1 SPT để thực hiện các thử nghiệm chức năng của SPT. Các mẫu thử được cung cấp phải đại diện (xét về mặt kết cấu và các cài đặt) cho dây chuyền sản xuất bình thường của nhà sản xuất và phải bao gồm cả các tùy chọn.

9.2.2.4.2 Nếu cung cấp nhiều mẫu để thử nghiệm môi trường, các thử nghiệm có thể được chia giữa các mẫu và thực hiện theo bất kỳ thứ tự nào.

Ghi chú:

Ví dụ 1. Nếu có 2 mẫu được cung cấp để làm thử nghiệm về môi trường, thì các thử nghiệm về vận hành phải được thực hiện trên mẫu thử đầu tiên, việc thử nghiệm đó không cần phải thực hiện theo thứ tự định trước nào, tiếp theo sau là một phép thử nào đó trong số các phép thử về độ bền. Những phép thử về độ bền khác được thực hiện trên mẫu thử thứ 2. Phải tiến hành thử nghiệm về chức năng cả trước và sau mỗi phép thử nghiệm về môi trường.

Ví dụ 2. Nếu có 3 mẫu được cung cấp để làm thử nghiệm về mặt môi trường, thì một mẫu được thử tất cả các thử nghiệm về vận hành, việc thử nghiệm đó không cần phải thực hiện theo thứ tự định trước nào. Mẫu thứ 2 sẽ được thử một phép thử nào đó trong số các phép thử về độ bền. Những phép thử về độ bền khác được thực hiện trên mẫu thử thứ 3. Phải tiến hành thử nghiệm về chức năng cả trước và sau mỗi thử nghiệm về môi trường.

9.3 Kiểm tra, thử nghiệm RCT

9.3.1 Chuẩn bị thử nghiệm

9.3.1.1 Điều kiện thử nghiệm

Nhiệt độ: 15 °C đến 35 °C;

Độ ẩm tương đối: 25% đến 75%;

Áp suất khí quyển: 86 kPa đến 106 kPa.

9.3.1.2 Lắp đặt

RCT sẽ được lắp đặt theo hướng dẫn lắp đặt của nhà sản xuất . Bất kỳ thiết bị bổ sung nào cần thiết để thực hiện các thử nghiệm (VÍ DỤ: mô phỏng ATS và SPT) sẽ được nhà sản xuất cung cấp theo thỏa thuận với đơn vị thử nghiệm.

9.3.1.3 Nguồn điện cấp

Nguồn diện cung cấp cho RCT phải đáp ứng yêu cầu kỹ thuật theo hướng dẫn của nhà sản xuất

9.3.2 Yêu cầu chung

9.3.2.1 Mục đích của các thử nghiệm chức năng là để chứng minh rằng RCT thực hiện các chức năng cần thiết của nó. Nhà sản xuất phải cung cấp một hệ thống thiết lập kiểm tra đầy đủ chức năng, đảm bảo rằng toàn bộ các bài kiểm tra có thể được thực hiện một cách chính xác và toàn diện. Nhà sản xuất phải cung cấp một thiết lập thử nghiệm chức năng đầy đủ. Các thành phần của ATS như FDAD, SPT và mạng truyền có thể được cung cấp như thiết bị mô phỏng và/hoặc mạng giả lập để kiểm tra mà không cần sử dụng hệ thống thực tế.

9.3.2.2 Nếu thiết bị được hỗ trợ nhiều loại đường truyền đơn (single path) hoặc đường truyền kép (dual path), thì chỉ cần kiểm tra các loại đường truyền có yêu cầu khắt khe nhất. Yêu cầu về thời gian báo cáo tối đa sẽ được thử nghiệm cho từng đường truyền riêng lẻ.

9.3.2.3 Tất cả các giao diện mạng mà thiết bị sử dụng để truyền tin và tất cả các giao diện kết nối với AMS phải được kiểm tra để bảo đảm rằng RCT có thể giao tiếp với hệ thống một cách hiệu quả.

9.3.2.4 Các bài kiểm tra được trình bày tóm tắt tại Bảng 7, chương trình kiểm tra cụ thể được quy định tại phụ lục E

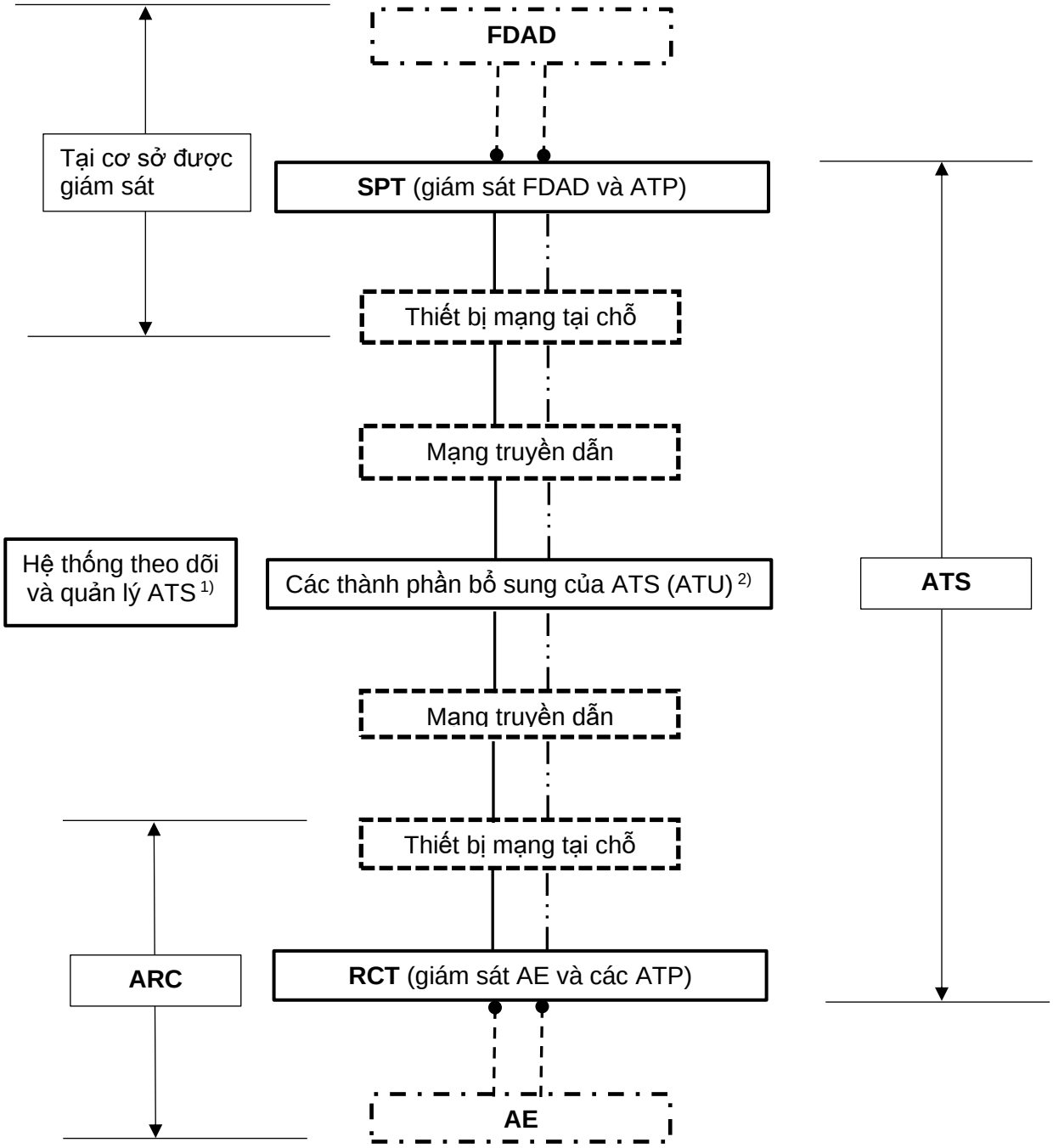
Bảng 7. Tóm tắt các bài kiểm tra chức năng của RCT

Điều, khoản	Yêu cầu kiểm tra	Mục tiêu kiểm tra/đánh giá	Phương pháp
7.1	Xử lý tín hiệu báo động	Chứng minh khả năng của RCT trong việc nhận, xử lý và chuyển tiếp tín hiệu thông báo cảnh báo hoặc báo động từ ATS.	Kiểm tra (mục 7. Phụ lục E)
7.2 và phụ lục C	Cấp quyền truy cập	Chứng minh rằng tất cả các mức truy cập đều tồn tại.	Kiểm tra (mục 1. Phụ lục A)
7.3	Tải lên và tải xuống phần mềm	Chứng minh rằng RCT có thể khôi phục sau một lần tải lên/tải xuống phần mềm không thành công.	Kiểm tra (mục 2. Phụ lục E)
7.4	Lưu trữ tham số và dữ liệu cụ thể	Chứng minh rằng RCT không mất bất kỳ tham số hoặc dữ liệu cụ thể nào sau khi đặt lại hoặc mất điện.	Kiểm tra (mục 3. Phụ lục E)
7.5	Giám sát và thông báo lỗi	Chứng minh rằng RCT thông báo lỗi ATS tới AMS như được quy định tại 7.5	Kiểm tra (mục 4. Phụ lục E)
7.6	Giao diện tới AMS	Chứng minh rằng các giao diện tới AMS được giám sát.	Kiểm tra (mục 5. Phụ lục E)

Điều, khoản	Yêu cầu kiểm tra	Mục tiêu kiểm tra/đánh giá	Phương pháp
7.7	Tín hiệu lỗi	Chứng minh rằng RCT phải báo hiệu lỗi theo tài liệu công bố của nhà sản xuất RCT.	Kiểm tra (mục 6. Phụ lục E)
7.8	Ghi lại sự kiện	Chứng minh rằng tất cả các sự kiện bắt buộc được ghi lại theo yêu cầu trong Bảng 4	Kiểm tra (mục 8. Phụ lục E)
	Độ chính xác và đồng bộ hóa đồng hồ	Chứng minh rằng dấu thời gian trong nhật ký sự kiện đáp ứng yêu cầu tại 7.8	Kiểm tra (mục 9. Phụ lục E)
	Độ bền của nhật ký	Xác minh tài liệu của nhà sản xuất chỉ rõ cách đảm bảo nhật ký có tuổi thọ 3 năm.	Xác thực (mục 10. Phụ lục E)
	Phương pháp tối ưu hóa lưu trữ sự kiện (nếu có)	Chứng minh rằng việc lưu trữ sự kiện được nhóm lại theo yêu cầu tại 7.8 là phù hợp.	Kiểm tra (mục 11. Phụ lục E)
	Nhận dạng người dùng trong nhật ký	Chứng minh rằng nhận dạng người dùng được ghi trong nhật ký phù hợp với yêu cầu tại Bảng 4	Kiểm tra (mục 12. Phụ lục E)
7.9	Chế độ vận hành	Chứng minh rằng các chế độ vận hành được thực hiện đáp ứng các yêu cầu tại 7.9	Kiểm tra (mục 13. Phụ lục E)
7.10	Tấn công từ chối dịch vụ	Xác minh tài liệu của nhà sản xuất RCT.	Xác thực (mục 14. Phụ lục E)
7.11	Bảo mật thông tin	Xác minh tuyên bố của nhà sản xuất về cách thực hiện bảo mật thông tin phù hợp với các yêu cầu.	Xác thực (mục 15. Phụ lục E)
7.12	Bảo mật chống giả mạo	Xác minh tuyên bố của nhà sản xuất về cách đảm bảo chống giả mạo phù hợp với các yêu cầu.	Xác thực (mục 15. Phụ lục E)
7.13	Dự phòng RCT	Xác minh rằng trong cấu hình ATS đường dẫn kép, lỗi một RCT không ảnh hưởng đến ATS	Kiểm tra (mục 16. Phụ lục E)
7.14	Tài liệu	Xác minh tài liệu của nhà sản xuất theo yêu cầu tại 7.14	Xác thực (mục 17. Phụ lục E)
7.15	Ghi nhãn	Xác minh đánh dấu và nhận diện theo yêu cầu tại 7.15	Xác thực
Ghi chú: Kiểm tra: Là các bài kiểm tra thử nghiệm vận hành thực tế để chứng minh rằng thiết bị đáp ứng yêu cầu; Đánh giá: Là việc kiểm tra tài liệu của nhà sản xuất để đảm bảo việc đáp ứng các yêu cầu			

Phụ lục A

(Tham khảo)



Ghi chú:

: Được cung cấp bởi ATSP

: Được kiểm soát một phần bởi ATSP

: Ngoài phạm vi của tiêu chuẩn

Đường truyền báo động (chính)

: Kết nối được giám sát giữa ATS và các nút cuối AE/ FDAD

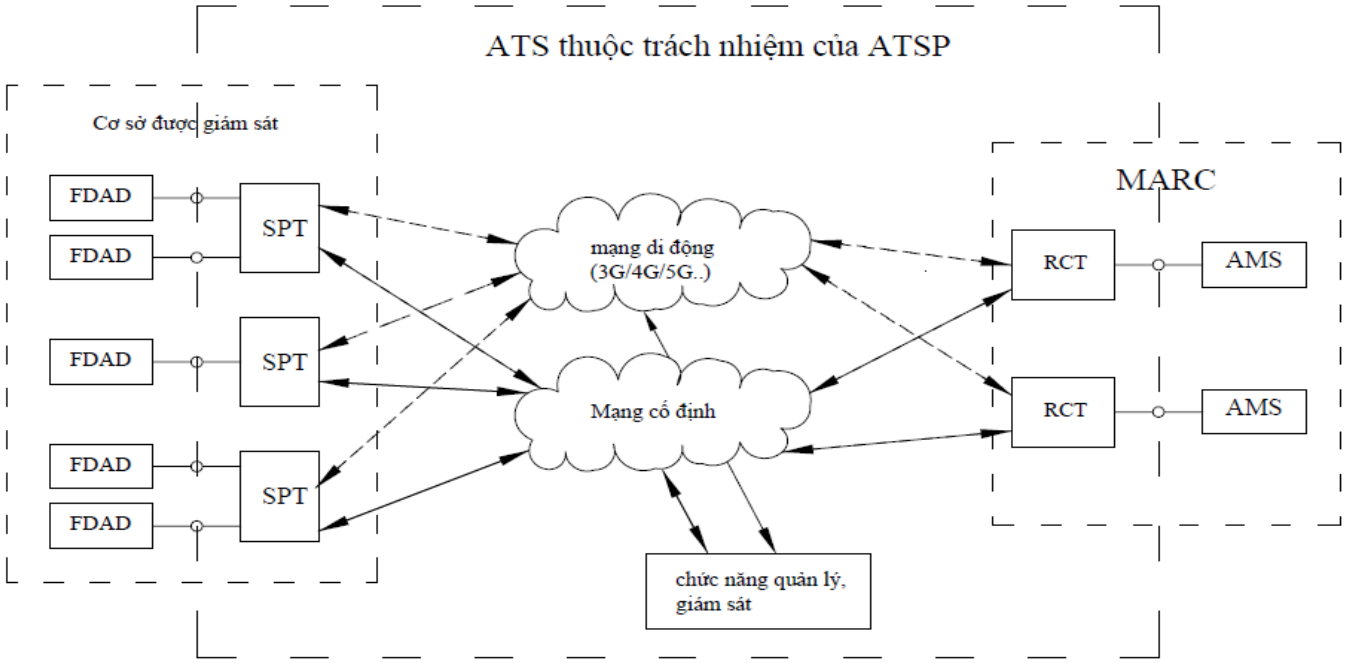
: Điểm cuối của ATP

1) : Cần thiết cho sự hoạt động của ATS, nhưng không mang ATP

2) : Không bắt buộc, nhưng nếu có thì mang theo ATP

Đường truyền báo động dự phòng: Có thể từ một giao diện mạng khác của SPT và kết thúc tại cùng RCT hoặc một RCT khác so với ATP chính, sử dụng cùng một mạng truyền tải hoặc một mạng truyền tải khác so với ATP chính

Hình A.1: Biểu diễn cấu trúc logic của ATS

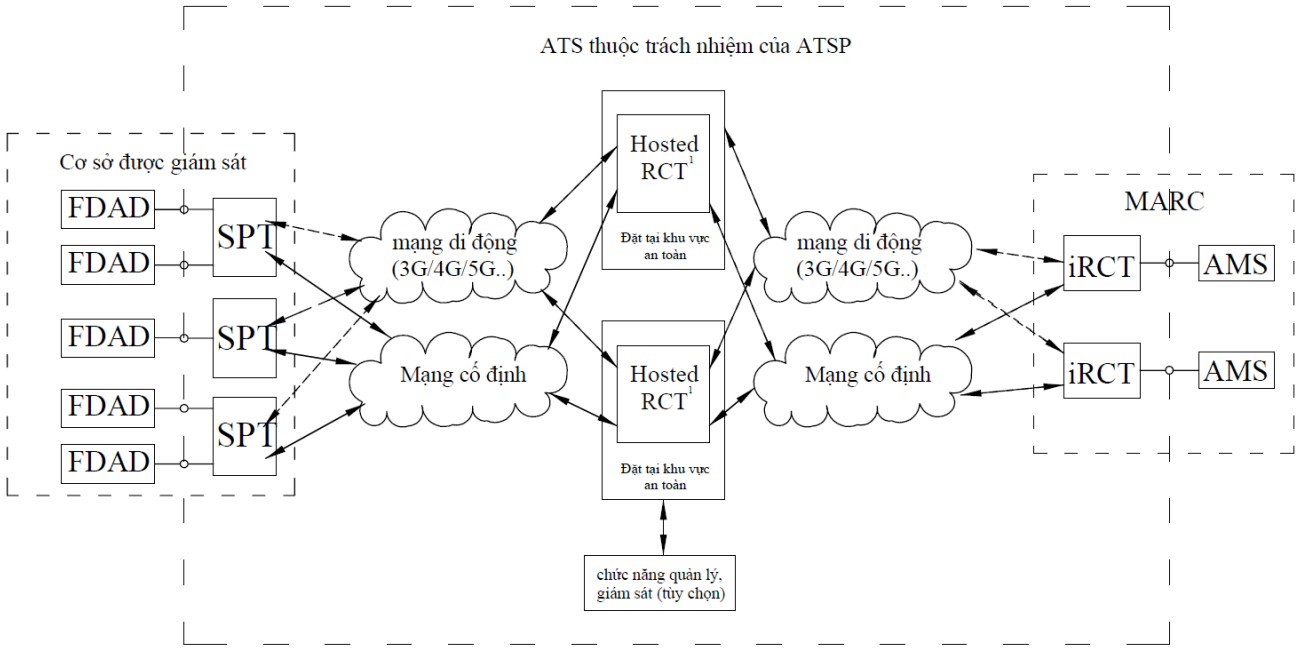


Ghi chú:

Đường truyền chính

Đường truyền dự phòng

Hình A.2. Minh họa ATS không được lưu trữ



Ghi chú:

: Đường truyền chính

: Đường truyền dự phòng

[1] : Có hoặc không có chức năng quản lý, giám sát

Hình A.3. Minh họa ATS được lưu trữ

Phụ lục B

(Tham khảo)

Tính khả dụng

1 Tổng quan

1.1 ATSP chịu trách nhiệm đo lường và báo cáo tính khả dụng của nhóm các ATS theo định nghĩa tại 3.1.25 và 3.1.29. Tính khả dụng là tỷ lệ phần trăm thời gian mà ATS hoạt động đáp ứng các yêu cầu của tiêu chuẩn này. Đây là tiêu chí hiệu suất rất quan trọng đối với chất lượng của Hệ thống truyền tin báo sự cố**.**

1.2 Nếu ATS hoặc ATP hoạt động đảm bảo trong mọi giây của mỗi ngày, tính khả dụng của nó sẽ là 100%, nếu không hoạt động bất kỳ thời gian nào, tính khả dụng là 0%. Con số tính khả dụng là 99,8% tức là có 0,2% không khả dụng, tương đương không hoạt động 20,16 phút trong bảy ngày (10.080 phút).

1.3 Có mối liên hệ trực tiếp giữa ATS và tính khả dụng của ATSN.

Ví dụ 1: Trong ATSN, sự cố mất điện 20 phút trong một tuần ảnh hưởng đến 10% tất cả các loại ATS cùng loại, dẫn đến khả năng sử dụng của ATSN là 99,989%. Do đó, yêu cầu về khả năng sử dụng của ATSN cao hơn nhiều so với yêu cầu về khả năng sử dụng của lẻ ATS.

Ví dụ 2: Bất kỳ sự cố nào làm mất điện của bất kỳ đường truyền mạng nào trong 17 giờ (trong một năm), ảnh hưởng đến tất cả các FDAD sẽ dẫn đến khả năng sử dụng của ATSN là 99,8%.

1.4 Việc đo lường tính khả dụng của ATS khác với tính khả dụng thường được các nhà điều hành mạng chỉ định. Tính khả dụng của ATS tại tiêu chuẩn này quy định tính khả dụng đầu cuối của hệ thống truyền tin báo sự cố, trong khi tính khả dụng của mạng thường chỉ xác định tính khả dụng của mạng. Tính khả dụng của mạng trái ngược với tính khả dụng của ATS thường không bao gồm các sự cố mất điện do bảo trì theo kế hoạch và không theo kế hoạch.

2 Tính khả dụng của ATS

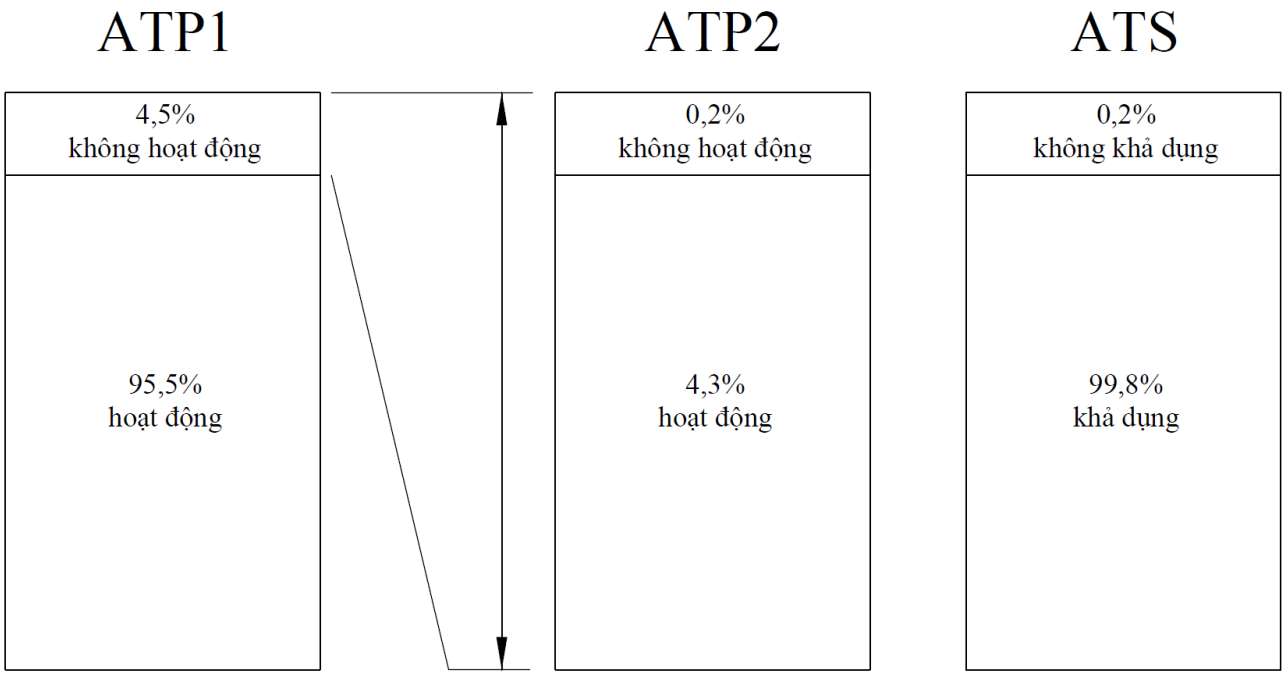
2.1 Khi một đường dẫn của ATS đường dẫn kép bị hỏng hoàn toàn nhưng một đường còn lại vẫn hoạt động bình thường, ATS vẫn được xem là khả dụng. Trong trường hợp lỗi này, nếu lỗi hỏng một đường dẫn vẫn tiếp diễn, ATS sẽ hoạt động như ATS đường dẫn đơn và bất kỳ mất kết nối nào trên đường dẫn còn lại (đường dẫn đang hoạt động) sẽ làm giảm tính khả dụng xuống dưới 100%

2.2 Mục tiêu tính khả dụng của ATS là 99,8% trong khoảng thời gian một tuần. Một tuần có 168 giờ nên thời gian không hoạt động tối đa được chấp nhận cho ATS ở mức khả dụng 99,8% là 20 phút. Để đáp ứng các mục tiêu khả dụng hàng tuần này, điều quan trọng là phải xem xét loại công nghệ đường truyền, môi trường cục bộ và khoảng cách ước tính từ cơ sở đến tổng đài hoặc trạm gốc vô tuyến. Các thỏa thuận mức dịch vụ phù hợp (thời gian sửa chữa) cũng nên được xem xét.

2.3 Trong tiêu chuẩn này, các ATS được quy định là loại đường dẫn kép, do đó khả năng hoạt động của từng đường dẫn (ATP) riêng lẻ có thể thấp hơn so với khả năng hoạt động (tính khả dụng) của ATS tổng thể. Ví dụ minh họa phương pháp đạt được tính khả dụng 99,8% của ATS được trình bày tại 2.4

2.4 Ví dụ về cách đạt được tính khả dụng của ATS là 99,8%, được minh họa ở hình B.1

ATP1 có khả năng sử dụng 95,5% và không khả dụng 4,5% (tình trạng lỗi); trong khoảng thời gian 4,5% khi ATP1 gặp lỗi, ATP2 hoạt động có khả năng sử dụng 95,5% và không khả dụng 4,5%. Với chu kỳ lỗi của ATP1 (4,5%) được ATP2 bao phủ với khả năng sử dụng 95,5%, chu kỳ lỗi dự kiến từ cả hai đường dẫn giảm xuống còn 0,2%, cung cấp khả năng sử dụng kết hợp là 99,8%.



Hình B.1. Minh họa về tính khả dụng của ATS

Phụ lục C

(Quy định)

Mức truy cập

Tiêu chuẩn này quy định bốn mức truy cập dựa trên khả năng người dùng truy cập vào chức năng của thiết bị. Các mức truy cập được phân loại dựa trên quyền truy cập logic (các chức năng hệ thống) và vật lý (tiếp cận thiết bị). Có 4 mức truy cập được quy định tại tiêu chuẩn này, cụ thể:

1. Mức truy cập 1: Truy cập cơ bản.

Truy cập logic bao gồm quyền xem các chỉ báo thông tin trạng thái cơ bản của hệ thống. Không thực hiện được bất kỳ thay đổi nào về cấu hình hoặc chức năng.

Truy cập vật lý bao gồm việc vận hành các chỉ báo và nút bấm thủ công mà không cần xác thực. Việc vận hành này không cần các công cụ đặc biệt

Người dùng dự kiến ở mức truy cập này có thể là thành viên cộng đồng hoặc nhân viên chịu trách nhiệm phản ứng ban đầu với các sự kiện (báo động, báo lỗi…)

2. Mức truy cập 2: Truy cập vận hành.

Truy cập logic bao gồm việc truy cập vào trạng thái hoạt động và các chức năng vận hành. Ở mức truy cập này có thể xem trạng thái hoạt động của hệ thống và thực hiện các chức năng liên quan đến việc cài đặt, cấu hình cơ bản của hệ thống.

Truy cập vật lý bao gồm quyền tiếp cận các thiết bị hoặc bảng điều khiển để thực hiện các chức năng vận hành cơ bản. Việc truy cập được bảo vệ bằng các công cụ bảo vệ đơn giản như: Khóa cơ, thẻ truy cập, bàn phím và mã hóa.

Người dùng dự kiến ở mức truy cập này có thể là nhân viên vận hành đã được đào tạo cơ bản

3. Mức truy cập 3: Truy cập bảo trì và cấu hình.

Truy cập logic bao gồm quyền truy cập vào các chức năng bảo trì, cấu hình chi tiết và các dữ liệu riêng cụ thể.

Truy cập vật lý bao gồm khả năng tiếp cận trực tiếp thiết bị, ệ thống để thực hiện truy cập logic mức 3

Người dùng dự kiến ở mức truy cập này có thể là nhân viên kỹ thuật viên có kỹ năng được phép thực hiện bảo trì và vận hành chi tiết theo hướng dẫn nhà sản xuất

4. Mức truy cập 4: Truy cập cập nhật phần mềm và bảo mật cao nhất.

Truy cập logic bao gồm quyền truy cập cập nhật phần mềm hệ thống hoặc chỉ đọc các tham số hệ thống mà không thể thay đổi chúng.

Truy cập vật lý bao gồm khả năng tiếp cận trực tiếp thiết bị, hệ thống để thực hiện các truy cập logic mức 4

Người dùng dự kiến ở mức truy cập này có thể là kỹ thuật viên được nhà sản xuất ủy quyền, có khả năng sửa chữa hoặc thay đổi phần mềm kiểm soát hệ thống

Phụ lục D

(Quy định)

Chương trình kiểm tra thiết bị thu phát tại trung tâm được giám sát (SPT)

1 Kiểm tra chức năng

1.1 Kiểm tra hoạt động của SPT

1.1.1 Mục đích của thử nghiệm

Mục đích của thử nghiệm là chứng minh khả năng của SPT theo quy định tại 6.1.1, 6.1.2, 6.1.3, 6.1.7 và 6.2.6 trong việc tiếp nhận, chuyển tiếp tín hiệu, chỉ báo trạng thái và tạo ra các thông báo cảnh báo.

1.1.2 Nguyên tắc

Thử nghiệm bao gồm việc tạo ra các tín hiệu báo động và báo lỗi quy định tại 6.1.1.1, sau đó xem xét chúng có được SPT tiếp nhận, tạo ra thông báo, chỉ báo trạng thái và truyền tới RCT một cách phù hợp.

Bảng D.1 — Thử nghiệm hoạt động của SPT

Bước	Điều kiện thử nghiệm	Quy trình thử nghiệm	Đo lường	Tiêu chí đạt
1.	FDAD được kết nối với SPT. ATS được cấu hình và hoạt động bình thường. RCT có sẵn hoặc mô phỏng được lắp đặt và hoạt động đầy đủ.	FADA ở trạng thái tĩnh lặng và ATS hoạt động bình thường	Kiểm tra chỉ báo trạng thái của SPT	SPT phải chỉ báo trạng thái theo quy định tại 6.1.2 và 6.2.6
2.	Như trên.	Kích hoạt và đặt lại tín hiệu cảnh báo cháy từ FDAD	- Kiểm tra SPT chỉ báo trạng thái SPT - Kiểm tra tín hiệu xác nhận có được gửi từ SPT tới FDAD không - Kiểm tra tín hiệu cảnh báo cháy có được tiếp nhận tại RCT không	- SPT phải chỉ báo trạng thái theo quy định tại 6.1.2 và 6.2.6. - Tín hiệu xác nhận phải được truyền đến FDAD sau khi SPT nhận được báo động thành công. - Tín hiệu cảnh báo cháy phải được SPT gửi tới RCT. SPT phải hiện thị trạng thái theo quy định tại 6.1.2 và 6.2.6 khi đã nhận được tín hiệu xác nhận từ RCT

Bước	Điều kiện thử nghiệm	Quy trình thử nghiệm	Đo lường	Tiêu chí đạt
3.	FDAD được kết nối với SPT. ATS không được kết nối (đảm bảo không có khả năng truyền báo động giữa SPT và RCT).	Kích hoạt tín hiệu cảnh báo cháy từ FDAD	- Kiểm tra chỉ báo trạng thái của SPT - Kiểm tra tín hiệu xác nhận có được gửi từ SPT tới FDAD không. Khi sử dụng giao diện song song, đầu ra SPT phải thể hiện lỗi như quy định tại 1.3.2 phụ lục F	- SPT phải chỉ báo trạng thái theo quy định tại 6.1.2 và 6.2.6. - Tín hiệu xác nhận phải được truyền đến FDAD sau khi SPT nhận được tín hiệu cảnh báo cháy thành công.
4.	Như trên	Tắt và khởi động lại SPT; khôi phục hoạt động bình thường của ATS	Xem báo động cháy được kích hoạt tại bước 3 có nhận được tại RCT không và không có tín hiệu xác nhận bổ sung nào nhận được từ FDAD.	SPT không truyền bất kỳ tín hiệu xác nhận giả mạo nào tới FDAD do nỗ lực truyền cảnh báo không thành công trước đó.
5.	FDAD được kết nối với SPT. ATS được cấu hình và hoạt động bình thường. RCT có sẵn hoặc mô phỏng được lắp đặt và hoạt động đầy đủ.	Kích hoạt tín hiệu cảnh báo cháy từ FDAD và ngắt kết nối ATS sau khi báo động được truyền đến SPT. Đảm bảo rằng báo động không được RCT nhận và/hoặc xác nhận.	- Kiểm tra chỉ báo trạng thái của SPT - Kiểm tra tín hiệu xác nhận có được gửi từ SPT tới FDAD không. Khi sử dụng giao diện song song, đầu ra SPT phải thể hiện lỗi như quy định tại 1.3.2 phụ lục F	- SPT phải chỉ báo trạng thái theo quy định tại 6.1.2 và 6.2.6. - Tín hiệu xác nhận phải được truyền đến FDAD sau khi SPT nhận được tín hiệu cảnh báo cháy thành công.
6.	Như trên	Tắt và khởi động lại SPT; khôi phục hoạt động bình thường của ATS	Xem báo động cháy được kích hoạt tại bước 5 có nhận được tại RCT không và không có tín hiệu xác nhận bổ sung nào nhận được từ FDAD.	SPT không truyền bất kỳ tín hiệu xác nhận giả mạo nào tới FDAD do nỗ lực truyền cảnh báo không thành công trước đó.
7.	Lặp lại từ bước 2 đến bước 6 lần lượt với các tín hiệu báo động từ FDAD (cảnh báo lỗi, giám sát, tắt, kiểm tra)	Lặp lại từ bước 2 đến bước 6	Lặp lại từ bước 2 đến bước 6	Như bước 2 đến bước 6 đối với mỗi tín hiệu báo động từ FDAD

Bước	Điều kiện thử nghiệm	Quy trình thử nghiệm	Đo lường	Tiêu chí đạt
8.	FDAD được kết nối với SPT. ATS được cấu hình và hoạt động bình thường. RCT có sẵn hoặc mô phỏng được lắp đặt và hoạt động đầy đủ.	Ngắt kết nối và khôi phục FDAD và SPT	- Kiểm tra chỉ báo trạng thái của SPT - Kiểm tra tín hiệu thông báo cảnh báo có được SPT tạo ra và truyền đến RCT/AE không	- SPT phải chỉ báo trạng thái theo quy định tại 6.1.2 và 6.2.6. - Tín hiệu thông báo cảnh báo được SPT tạo ra và truyền đến RCT/AE
9.	Như trên	Ngắt kết nối ATP chính và khôi phục	- Kiểm tra chỉ báo trạng thái của SPT - Kiểm tra tín hiệu thông báo cảnh báo có được SPT tạo ra và truyền đến RCT/AE không	- SPT phải chỉ báo trạng thái theo quy định tại 6.1.2 và 6.2.6. - Tín hiệu thông báo cảnh báo được SPT tạo ra và truyền đến RCT/AE
10.	Như trên	Ngắt kết nối ATP dự phòng và khôi phục	- Kiểm tra chỉ báo trạng thái của SPT - Kiểm tra tín hiệu thông báo cảnh báo có được SPT tạo ra và truyền đến RCT/AE không	- SPT phải chỉ báo trạng thái theo quy định tại 6.1.2 và 6.2.6. - Tín hiệu thông báo cảnh báo được SPT tạo ra và truyền đến RCT/AE
11.	Như trên	Lỗi nguồn điện chính và khôi phục	- Kiểm tra chỉ báo trạng thái của SPT - Kiểm tra tín hiệu thông báo cảnh báo có được SPT tạo ra và truyền đến RCT/AE không	- SPT phải chỉ báo trạng thái theo quy định tại 6.1.2 và 6.2.6. - Tín hiệu thông báo cảnh báo được SPT tạo ra và truyền đến RCT/AE
12.	Như trên	Lỗi nguồn điện dự phòng và khôi phục	- Kiểm tra chỉ báo trạng thái của SPT - Kiểm tra tín hiệu thông báo cảnh báo có được SPT tạo và truyền đến RCT/AE không	- SPT phải chỉ báo trạng thái theo quy định tại 6.1.2 và 6.2.6. - Tín hiệu thông báo cảnh báo được SPT tạo ra và truyền đến RCT/AE
13.	FDAD được kết nối với SPT. ATS được cấu hình và hoạt động bình thường. RCT có sẵn hoặc mô phỏng được lắp đặt và hoạt động đầy đủ.	Kích hoạt lần lượt các tín hiệu giám sát, tắt, kiểm tra, báo lỗi và cảnh báo cháy từ FDAD	- Kiểm tra chỉ báo trạng thái của SPT - Kiểm tra tín hiệu xác nhận được gửi từ SPT tới FDAD.	- SPT phải ưu tiên chỉ báo trạng thái báo động cháy theo quy định tại 6.1.2 và 6.2.6. - Tín hiệu từ SPT truyền đến RCT phải ưu tiên tín hiệu báo cháy.

1.2 Báo cáo lỗi ATS cho FDAD

1.2.1 Mục đích của bài kiểm tra

Mục đích của bài kiểm tra là chứng minh khả năng của SPT trong việc báo cáo lỗi ATS cho FDAD theo quy định tại 6.1.4

1.2.2 Nguyên tắc

Bài kiểm tra bao gồm việc đánh giá từng ATP và ATS để kiểm tra việc báo cáo lỗi ATS cho FDAD trong thời gian báo cáo được quy định tại 6.1.4.

Ghi chú: Việc tháo cáp Ethernet hoặc ăng-ten không phải là một thử nghiệm phù hợp. Điều này chỉ giám sát giao diện mạng như đo điện áp đường dây cho các đường dây tương tự. Nhà sản xuất sẽ chỉ định trong tài liệu cách thực hiện thử nghiệm

Bảng D.2 – Thử nghiệm báo cáo lỗi ATS cho FDAD

Bước	Điều kiện thử nghiệm	Quy trình thử nghiệm	Đo lường	Tiêu chí đạt
1	SPT và mọi thiết bị cần thiết cho phép SPT hoạt động theo yêu cầu phải được lắp đặt và ở trạng thái hoạt động. SPT được kết nối với ATP chính và dự phòng	Kiểm tra xem mỗi ATP có hoạt động bình thường không và đầu ra của FDAD có báo cáo ATP đang hoạt động không.	Ghi lại trạng thái hoạt động của FDAD (hoặc trình mô phỏng) liên quan.	Không được hiển thị lỗi.
2	Như bước 1	Mất kết nối ATP chính	Ghi lại trạng thái hoạt động của FDAD (hoặc trình mô phỏng) liên quan.	Không hiển thị lỗi ATS. Có thể hiển thị lỗi ATP.
3	Tiếp sau bước 2	Thất bại ATP thay thế.	Ghi lại thời gian SPT báo hiệu ATS bị lỗi. (có thể sử dụng thiết bị đo thời gian hoặc bằng FDAD)	Tình trạng lỗi ATS phải được hiển thị trong thời gian quy định tại 6.1.4
4	Như sau bước 3.	Phục hồi ATP chính và ATP thay thế.	Ghi lại trạng thái của FDAD (hoặc trình mô phỏng) được liên kết.	Không được hiển thị lỗi.

1.3 Giao diện với FDAD

1.3.1 Giao diện nối tiếp chuẩn hóa tới FDAD

1.3.1.1 Mục đích của thử nghiệm

Mục đích của thử nghiệm này là chứng minh rằng giao diện nối tiếp tới FDAD, nếu được triển khai, tuân thủ các yêu cầu của 6.1.5 và phụ lục G

1.3.1.2 Nguyên tắc

Thử nghiệm bao gồm việc tuân theo các tài liệu hướng dẫn của nhà sản xuất để cài đặt SPT. Do đó, việc giám sát và hiệu suất của liên kết này được thử nghiệm.

Bảng D.3 — Thử nghiệm giao diện nối tiếp chuẩn hóa tới FDAD

Bước	Điều kiện thử nghiệm	Quy trình thử nghiệm	Đo lường	Tiêu chí đạt
1	SPT và mọi thiết bị cần thiết cho phép SPT hoạt động theo yêu cầu phải được lắp đặt và ở trạng thái hoạt động.	Kết nối SPT với FDAD thông qua giao diện nối tiếp như được chỉ định trong tài liệu sản phẩm.	Ghi lại xem việc kết nối SPT với FDAD có phù hợp với tài liệu hay không.	Việc kết nối SPT và FDAD phải tuân theo tài liệu hướng dẫn.
2	Như trên	Tạo tín hiệu báo động trên FDAD.	Ghi lại thời gian truyền theo 6.1.5.1	Thời gian truyền phải đáp ứng quy định tại 6.1.5.1
3	Như trên	Ngắt kết nối giao diện nối tiếp.	Ghi lại thời gian báo cáo: Thời gian từ khi ngắt kết nối đến khi tín hiệu ngắt kết nối được chỉ định trên RCT	Thời gian báo cáo phải đáp ứng quy định tại 6.1.5.1 (không vượt quá 90 s).

1.3.2 Giao diện song song chuẩn hóa tới FDAD

1.3.2.1 Mục đích của thử nghiệm

Mục đích của thử nghiệm là chứng minh khả năng của SPT theo quy định tại 6.1.5 và Phụ lục G để cung cấp kết nối được giám sát tới FDAD liên quan thông qua giao diện song song chuẩn hóa nếu được triển khai.

1.3.2.2 Nguyên tắc

Thử nghiệm bao gồm việc cố gắng sử dụng giao diện song song tới FDAD liên quan theo Phụ lục G. Thử nghiệm thực hiện truyền cảnh báo, lỗi giao diện và xác nhận cảnh báo thông qua giao diện song song tới FDAD.

Bảng D.4 - Thử nghiệm giao diện song song chuẩn hóa tới FDAD

Bước	Điều kiện thử nghiệm	Quy trình thử nghiệm	Đo lường	Tiêu chí đạt
1	SPT và FDAD (hoặc một trình mô phỏng giao diện FDAD tương đương) được kết nối thông qua giao diện FDAD song song và đang hoạt động theo yêu cầu. SPT được kết nối với ATS hoạt động đầy đủ.	Một báo động sẽ được FDAD kích hoạt tới mọi đầu vào báo động song song của SPT theo yêu cầu của Phụ lục G.	Ghi lại nếu sự thay đổi ± 40% giá trị điện trở tĩnh được nhận dạng là báo động và được truyền đến giao diện mạng SPT.	Sự thay đổi lớn hơn ± 40% so với giá trị điện trở tĩnh được coi là báo động.
2	Như trên	Lỗi FDAD hoặc thông báo khác được FDAD kích hoạt đối với mọi thông báo/lỗi đầu vào của SPT theo yêu cầu của Phụ lục A.	Ghi lại nếu sự thay đổi từ trở kháng dưới 100Ω thành trên 500 kΩ trong thời gian dài hơn 200 ms được nhận biết là sự thay đổi trạng thái từ bình thường sang trạng thái hoạt động.	Sự thay đổi trở kháng từ dưới 100Ω lên trên 500 kΩ được nhận biết là sự thay đổi trạng thái của đầu vào thông báo/lỗi của SPT.
3	Như trên	ATS không khả dụng.	Theo dõi trạng thái đầu ra lỗi SPT (1.3.2 phụ lục G) đến FDAD	Đầu ra lỗi SPT (1.3.2 phụ lục G) sẽ thay đổi trạng thái trong thời gian báo cáo phù hợp
4	Như trên	Kích hoạt tất cả các đầu ra SPT và kết nối nguồn 20mA vào tất cả các đầu ra riêng lẻ.	Ghi lại xem tất cả Đầu ra SPT có thể tiêu thụ 20mA trong trường hợp đầu ra được kích hoạt tới FDAD.	Tất cả đầu ra SPT tới FDAD có thể chịu được ít nhất 20mA.
5	Như trên	Làm thay đổi giao diện với FDAD bằng cách loại bỏ hoặc rút ngắn kết nối giao diện của SPT với FDAD.	Ghi lại nếu có thông báo báo động được tạo ra.	Phát hiện hành vi can thiệp vào kết nối SPT tới FDAD và báo cáo cho RCT.

1.3.3 Giao diện độc quyền tới FDAD

1.3.3.1 Mục đích của thử nghiệm

Mục đích của thử nghiệm này là chứng minh rằng giao diện độc quyền tới FDAD, nếu được triển khai, đáp ứng quy định tại 6.3.4.

1.3.3.2 Nguyên tắc

Thử nghiệm được thực hiện theo hướng dẫn của nhà sản xuất để cài đặt SPT. Do đó, việc giám sát và hiệu suất của liên kết này được thử nghiệm.

Bảng D.5 - Thử nghiệm giao diện độc quyền tới FDAD

Bước	Điều kiện thử nghiệm	Quy trình thử nghiệm	Đo lường	Tiêu chí đạt
1	SPT và mọi thiết bị cần thiết cho phép SPT hoạt động theo yêu cầu phải được lắp đặt và ở trạng thái hoạt động.	Kết nối SPT với FDAD theo chỉ định trong tài liệu sản phẩm.	Ghi lại xem việc kết nối SPT với FDAD có phù hợp với tài liệu hay không.	Việc kết nối SPT và FDAD phải tuân theo tài liệu hướng dẫn.
2	Như trên	Tạo tín hiệu báo động trên FDAD.	Ghi lại thời gian truyền theo 6.1.5.1	Thời gian truyền phải đáp ứng quy định tại 6.1.5.1
3	Như trên	Ngắt kết nối giao diện.	Ghi lại thời gian báo cáo: Thời gian từ khi ngắt kết nối đến khi tín hiệu ngắt kết nối được chỉ định trên RCT	Thời gian báo cáo phải đáp ứng quy định tại 6.1.5.1 (không vượt quá 90 s).

Ghi chú: Khuyến nghị nên thử nghiệm bằng cách tháo cáp Ethernet hoặc ăng-ten

1.4 Giám sát giao diện mạng truyền dẫn

1.4.1 1 Mục đích của thử nghiệm

Mục đích của thử nghiệm này là chứng minh rằng SPT có thể phát hiện lỗi ATP khi mỗi giao diện mạng truyền dẫn bị lỗi theo quy định tại 6.1.6

Ghi chú Ví dụ, có thể là cáp Ethernet hoặc kết nối mạng qua mạng di động.

1.4.2 Nguyên tắc

Thử nghiệm bao gồm việc ngắt kết nối các giao diện mạng SPT khỏi mạng và theo dõi xem có gửi thông báo lỗi đến RCT hay không.

Ghi chú: Khuyến nghị nên thử nghiệm bằng cách tháo cáp Ethernet hoặc ăng-ten.

Bảng D.6 - Thử nghiệm phát hiện lỗi ATP khi giao diện mạng truyền dẫn bị lỗi

Bước	Điều kiện thử nghiệm	Quy trình thử nghiệm	Đo lường	Tiêu chí đạt
1	SPT và mọi thiết bị cần thiết cho phép SPT hoạt động theo yêu cầu phải được lắp đặt và ở trạng thái hoạt động. RCT hoặc một thiết bị mô phỏng cung cấp đủ chức năng để giao tiếp với SPT.	Ngắt kết nối giao diện mạng đầu tiên (bước 1 và 2 sẽ được lặp lại cho tất cả các giao diện mạng)	Theo dõi xem lỗi ATP có được ghi vào không Nhật ký sự kiện. và tín hiệu lỗi có được gửi đến RCT không.	Lỗi ATP sẽ được ghi vào nhật ký sự kiện. Tín hiệu lỗi ATP sẽ được gửi đến RCT.
2		Kết nối lại giao diện mạng đã ngắt kết nối (bước 1 và 2 sẽ được lặp lại cho tất cả các giao diện mạng)	Theo dõi xem quá trình khôi phục ATP có được ghi vào nhật ký sự kiện và tín hiệu khôi phục có được gửi đến RCT không.	Quá trình khôi phục ATP sẽ được ghi vào nhật ký sự kiện. Tín hiệu khôi phục ATP sẽ được gửi đến RCT.

1.5 Mức độ truy cập

1.5.1 Mục đích của thử nghiệm

Mục đích của thử nghiệm là chứng minh khả năng của SPT đáp ứng theo quy định tại 6.1.8 và phụ lục C để cung cấp tối đa 4 mức độ truy cập và xác minh các quyền truy cập đó.

1.5.2 Nguyên tắc

Thử nghiệm bao gồm việc cố gắng sử dụng các chức năng và điều khiển theo yêu cầu của 6.1.8 và phụ lục C, vận hành SPT ở mỗi mức độ truy cập và xác minh rằng quyền truy cập được cấp cho các chức năng được phép và bị từ chối đối với các chức năng không được phép.

Bảng D.7 — Thử nghiệm mức độ truy cập

Bước	Điều kiện thử nghiệm	Quy trình thử nghiệm	Đo lường	Tiêu chí đạt
1	SPT và các thiết bị cần thiết được lắp đặt theo hướng dẫn, SPT được sử dụng lần đầu.	Bật SPT và giữ nguyên khóa mặc định.	Ghi lại nếu có thể hoàn thành việc đưa vào sử dụng.	Việc đưa vào vận hành sẽ không được hoàn tất.
2	SPT và mọi thiết bị cần thiết cho phép SPT hoạt động theo yêu cầu phải được lắp đặt và ở trạng thái hoạt động.	Ở mức truy cập 1, hãy thử vận hành tất cả các chức năng và điều khiển theo chỉ định của nhà sản xuất cho mức truy cập 1.	Ghi lại xem có được phép truy cập hay không.	Quyền truy cập tuân theo mục 6.1.8 và phụ lục C.

Bước	Điều kiện thử nghiệm	Quy trình thử nghiệm	Đo lường	Tiêu chí đạt
3	Như trên	Lặp lại như bước 1 cho mức truy cập 2.	Như trên	Như trên
4	Như trên	Lặp lại như bước 1 cho mức truy cập 3.	Như trên. Ghi lại nếu quyền truy cập mức 3 chỉ khả thi nếu được người dùng mức 2 cấp.	Như trên
5	Như trên	Cố gắng truy cập bằng cách nhập sai khóa lần trong khoảng thời gian 60 giây.	Ghi lại xem quyền truy cập có bị từ chối không.	Không được phép truy cập.
6	Trạng thái sau bước 5	Chờ 80 giây (+/- 5 giây) và thử lại bằng khóa hợp lệ để được truy cập.	Ghi lại xem quyền truy cập có bị từ chối không.	Không được phép truy cập.
7	Xem phương pháp của nhà sản xuất về chất lượng thuật toán được sử dụng để đạt được quyền truy cập từ xa với khóa có ít nhất 1.000.000 khả năng khác nhau.	Xem lại tài liệu.		Thuật toán có thể phân biệt được 1.000.000 khóa khác nhau.

1.6 Bảo mật chống giả mạo và bảo mật thông tin

1.6.1 Nhà sản xuất phải mô tả trong tài liệu SPT các phương pháp được sử dụng để bảo vệ chống lại việc thay thế SPT bằng thiết bị giống hệt hoặc thiết bị mô phỏng theo các yêu cầu được nêu trong 6.1.9.

1.6.2 Nhà sản xuất phải mô tả trong tài liệu SPT các phương pháp được sử dụng để bảo vệ thông tin được truyền bởi ATS nhằm ngăn chặn việc đọc trái phép và sửa đổi trái phép thông tin được truyền theo các yêu cầu được mô tả trong 6.1.10.

1.7 Tải lên và tải xuống phần mềm và chương trình cơ sở

1.7.1 Đối tượng của bài kiểm tra

Mục đích của thử nghiệm này là chứng minh rằng việc tải lên và tải xuống chương trình cơ sở của SPT, nếu được triển khai, tuân thủ các yêu cầu của 6.1.12.

1.7.2 Nguyên tắc

Thử nghiệm bao gồm việc cố gắng cập nhật chương trình cơ sở của SPT, vận hành SPT ở mức truy cập phù hợp và làm theo hướng dẫn trong sổ tay hướng dẫn SPT.

Bảng D.8 — Thử nghiệm tải lên và tải xuống phần mềm và chương trình cơ sở

Bước	Điều kiện thử nghiệm	Quy trình thử nghiệm	Đo lường	Tiêu chí đạt
1	SPT và mọi thiết bị cần thiết cho phép SPT hoạt động theo yêu cầu phải được lắp đặt và ở trạng thái hoạt động.	Ở mức truy cập 1, hãy thử áp dụng bản cập nhật chương trình cơ sở.	Ghi lại xem có được phép cập nhật chương trình cơ sở hay không.	Không được phép cập nhật chương trình cơ sở.
2	Như trên	Lặp lại như trên đối với mức truy cập 2.	Như trên	Như trên
3	Như trên	Lặp lại như trên đối với mức truy cập 3.	Như trên	Như trên
4	Như trên	Lặp lại như trên đối với mức truy cập 4.	Như trên	Có thể cập nhật chương trình cơ sở.
5	Như trên	Lặp lại như trên đối với mức truy cập 4. Ngắt kết nối mạng trong quá trình cập nhật chương trình cơ sở.	Ghi lại xem SPT có bị lỗi không hoặc hoạt động trở lại bình thường.	SPT sẽ hoạt động bình thường sau khi thử tải xuống chương trình cơ sở.

1.8 Lưu trữ thông số

1.8.1 Mục đích của thử nghiệm

Mục đích của thử nghiệm là chứng minh khả năng của SPT tuân thủ 6.1.13 để cung cấp khả năng miễn nhiễm khi lưu trữ thông số khi mất điện hoặc trình tự khởi động.

1.8.2 Nguyên tắc

Bài kiểm tra bao gồm việc thay đổi ít nhất 2 tham số cụ thể của trang web và đọc lại các tham số này sau một chu kỳ cấp nguồn (mất điện/phục hồi điện) và trình tự khởi động.

Bảng D.9 - Kiểm tra lưu trữ tham số

Bước	Điều kiện thử nghiệm	Quy trình thử nghiệm	Đo lường	Tiêu chí đạt
1	SPT và mọi thiết bị cần thiết cho phép SPT hoạt động theo yêu cầu phải được lắp đặt và ở trạng thái hoạt động.	Thay đổi và lưu ít nhất 2 dữ liệu riêng cụ thể theo quy trình trong hướng dẫn.	Ghi lại xem những thay đổi có được lưu trữ hay không.	
2	Như trên	Tắt nguồn SPT		
3	SPT ở trạng thái tắt nguồn	Chờ ít nhất 10 giây rồi bật lại SPT.	Ghi lại xem SPT có đang ở trạng thái hoạt động hay không.	SPT sẽ ở trạng thái hoạt động như trước khi cấp nguồn.
4	Giống như Bước 1	Đọc các thông số đã thay đổi theo đúng quy trình trong tài liệu hướng dẫn.	Ghi lại các giá trị tham số.	Các giá trị tham số phải giống như trước khi bật nguồn.

1.9 Ghi nhật ký sự kiện

1.9.1 Mục đích của thử nghiệm

Mục đích của thử nghiệm này là chứng minh rằng các sự kiện được ghi lại tại SPT theo yêu cầu trong Bảng 2.

1.9.2 Nguyên tắc

Thử nghiệm bao gồm việc tạo các sự kiện được yêu cầu trong Bảng 2, sau đó xem xét rằng chúng được ghi lại trong nhật ký sự kiện SPT.

Bảng D.10 - Thử nghiệm ghi nhật ký sự kiện

Bước	Điều kiện thử nghiệm	Quy trình thử nghiệm	Đo lường	Tiêu chí đạt
1	SPT và mọi thiết bị cần thiết cho phép SPT hoạt động theo yêu cầu phải được lắp đặt và ở trạng thái hoạt động.	Tạo từng sự kiện được liệt kê trong Bảng 2.	Kiểm tra xem tất cả các sự kiện có được ghi vào nhật ký sự kiện SPT theo danh mục hay không.	Tất cả các sự kiện đã triển khai sẽ được ghi lại trong nhật ký sự kiện SPT.

1.10 Bảo vệ nhật ký

1.10.1 Mục đích của thử nghiệm

Mục đích của thử nghiệm là xác nhận rằng nhật ký được bảo vệ chống lại việc xóa hoặc thay đổi nội dung nhật ký một cách vô tình hoặc cố ý.

1.10.2 Nguyên tắc

Việc xác nhận bao gồm việc xác minh phương pháp của nhà sản xuất đã nêu để đạt được sự tuân thủ với 6.1.14 và xác nhận nhật ký được bảo vệ chống lại việc xóa hoặc thay đổi một cách vô tình hoặc cố ý

1.11 Khả năng lưu trữ và độ bền của nhật ký sự kiện

1.11.1 Mục đích của thử nghiệm

Mục đích của thử nghiệm là chứng minh rằng nhật ký chứa tối thiểu các bản ghi sự kiện và tồn tại trong khoảng thời gian theo quy định tại 6.1.14.2.

1.11.2 Nguyên tắc

Thử nghiệm bao gồm việc tạo các bản ghi sự kiện nhật ký và xác nhận rằng số lượng và việc lưu trữ các bản ghi sự kiện đáp ứng các yêu cầu của 6.1.14.2.

Bảng D.11 - Thử nghiệm khả năng lưu trữ của nhật ký sự kiện

Bước	Điều kiện thử nghiệm	Quy trình thử nghiệm	Đo lường	Tiêu chí đạt
1	SPT và mọi thiết bị cần thiết cho phép SPT hoạt động theo yêu cầu phải được lắp đặt và ở trạng thái hoạt động.	Tạo 1000 sự kiện nhật ký theo 6.1.14.2	Kiểm tra xem tất cả các bản ghi sự kiện đã được ghi lại chưa.	Tất cả các bản ghi sự kiện đều được ghi lại chính xác.
2	Như trên	Tạo vượt quá 1000 sự kiện	Kiểm tra xem các sự kiện gần đây nhất đã được ghi lại chưa.	Các bản ghi sự kiện gần đây nhất được ghi lại một cách chính xác.
3	Như trên	Ngắt nguồn điện khỏi thiết bị trong 30 ngày sau đó cấp lại nguồn điện.	Kiểm tra xem có bản ghi sự kiện nào bị ảnh hưởng không.	Tất cả các bản ghi sự kiện vẫn được ghi lại chính xác.

1.12 Độ phân giải thời gian

1.12.1 Mục đích của bài kiểm tra

Mục đích của bài kiểm tra này là chứng minh rằng độ chính xác của dấu thời gian được đính kèm vào các sự kiện trong nhật ký tuân thủ các yêu cầu của 6.1.14.4

1.12.2 Nguyên tắc

Bài kiểm tra bao gồm việc tạo các sự kiện, trong khi xác minh dấu thời gian so với nguồn thời gian tham chiếu. Các bài kiểm tra sẽ được thực hiện so với tham chiếu thời gian được xác định rõ. Vì mục đích này, máy chủ NTP ở cấp độ Stratum 2 (thường có sẵn trên Internet) cung cấp độ chính xác cần thiết.

Bảng D.12 - Kiểm tra độ phân giải thời gian

Bước	Điều kiện thử nghiệm	Quy trình thử nghiệm	Đo lường	Tiêu chí đạt
1	SPT và mọi thiết bị cần thiết cho phép SPT hoạt động theo yêu cầu phải được lắp đặt và ở trạng thái hoạt động.	Tạo sự kiện.	Ghi lại dấu thời gian tạo sự kiện.	Phải có một bản nhật ký được ghi, với độ phân giải tối thiểu là một giây và độ lệch so với thời gian tham chiếu không quá 5 giây

1.13 Tài liệu

Để xác minh rằng tất cả các tài liệu bắt buộc đều được cung cấp đầy đủ và chính xác

1.14 Phương tiện để xác minh hiệu suất ATS

1.14.1 Mục đích của thử nghiệm

Mục đích của thử nghiệm này là chứng minh rằng các phương tiện được mô tả trong tài liệu có thể được sử dụng để đo thời gian truyền, thời gian báo cáo và tính khả dụng của ATS

1.14.2 Nguyên tắc

Thử nghiệm bao gồm việc tái tạo quy trình được mô tả trong tài liệu do nhà sản xuất cung cấp và kiểm tra xem quy trình này có cung cấp thước đo hiệu suất của ATS hay không.

Bảng D.13 - Thử nghiệm các phương tiện để xác minh hiệu suất ATS

Bước	Điều kiện thử nghiệm	Quy trình thử nghiệm	Đo lường	Tiêu chí đạt
1	ATS đang hoạt động đầy đủ và được cấu hình cho bất kỳ danh mục ATS nào.	Áp dụng quá trình được mô tả trong tài liệu để đo thời gian truyền.	Kiểm tra xem quy trình có cho phép đo 3 thời gian truyền theo quy định tại 5.3.2 Ước tính độ chính xác của phép đo.	Quá trình này sẽ cho phép đo 3 thời gian truyền theo quy định tại 5.3.2 Độ chính xác của phép đo không được thấp hơn 5% của mỗi một trong 3 thời gian truyền tối đa cần xác minh.
2	Như trên	Áp dụng quá trình được mô tả trong tài liệu để đo thời gian báo cáo.	Đối với loại DP SPT: Kiểm tra xem quy trình có cho phép đo 4 thời gian báo cáo như quy định tại bảng 1. Ước tính độ chính xác của phép đo.	Quá trình này sẽ cho phép đo thời gian báo cáo theo quy định tại bảng 1 Độ chính xác của phép đo không được thấp hơn 5% của mỗi một trong 3 thời gian truyền tối đa cần xác minh.

3	Như trên	Áp dụng quá trình được mô tả trong tài liệu để đo lường tính khả dụng của ATS và ATP.	Kiểm tra xem quy trình có cho phép đo lường tính khả dụng của ATS và ATP Ước tính độ chính xác của phép đo.	Quá trình này sẽ cho phép đo lường tính khả dụng của ATS và ATP Độ chính xác của phép đo phải phù hợp với số chữ số có nghĩa của mức khả dụng tối thiểu

2 Các thử nghiệm về môi trường

2.1 Điều kiện lạnh (vận hành)

2.1.1 Mục đích của phép thử

Mục đích của phép thử là để chứng minh khả năng thiết bị đảm bảo được đúng chức năng trong môi trường có điều kiện nhiệt độ thấp phù hợp với môi trường làm việc được dự định trước.

2.1.2 Quy trình thử nghiệm

2.1.2.1 Tổng quát

Sử dụng các quy trình thử nghiệm với sự thay đổi dần về nhiệt độ theo mô tả trong TCVN 7699-2-1 (IEC 60068-2-1). Sử dụng phép thử Ad cho các mẫu thử có tản nhiệt (như quy định trong TCVN 7699-2-1 (IEC 60068-2-1)) và sử dụng phép thử Ab cho các mẫu thử không có tản nhiệt.

2.1.2.2 Các phép đo ban đầu

Trước khi tác động điều kiện ổn định khi thử, thực hiện thử nghiệm về chức năng.

2.1.2.3 Tình trạng của mẫu thử trong điều kiện ổn định khi thử

Lắp mẫu thử theo quy định trong 9.2.1.2.2 và nối với nguồn cấp điện thích hợp, theo dõi và cấp điện vào mẫu (xem 9.2.1.2.3).

Mẫu thử phải ở trạng thái tĩnh lặng.

2.1.2.4 Điều kiện ổn định khi thử

Tác động điều kiện ổn định khi thử sau:

- Nhiệt độ: (-5 ± 3) °C hoặc mức nhiệt độ nhỏ nhất theo phân cấp;
- Thời gian 16 h

2.1.2.5 Các phép đo trong quá trình chịu tác động của điều kiện ổn định khi thử

Theo dõi mẫu thử trong suốt khoảng thời gian chịu tác động của điều kiện ổn định khi thử để phát hiện mọi thay đổi về tình trạng. Trong một giờ cuối của thời gian tác động môi trường, thực hiện thử nghiệm về chức năng của mẫu.

2.1.2.6 Các phép đo cuối

Sau khoảng thời gian để hồi phục, thực hiện thử nghiệm về chức năng của mẫu và kiểm tra mẫu bằng trực quan để phát hiện mọi hư hỏng về mặt cơ học ở cả bên trong và bên ngoài.

2.2 Điều kiện ẩm nhiệt, trạng thái ổn định (vận hành)

2.2.1 Mục đích của phép thử

Mục đích của phép thử là để chứng minh khả năng thiết bị đảm bảo được đúng chức năng trong điều kiện độ ẩm tương đối ở mức cao (không ngưng tụ) có thể xảy ra trong những khoảng thời gian ngắn trong môi trường làm việc.

2.2.2 Quy trình thử nghiệm

2.2.2.1 Tổng quát

Sử dụng quy trình thử nghiệm theo mô tả trong TCVN 7699-2-78 (IEC 60068-2-78).

2.2.2.2 Các phép đo ban đầu

Trước khi tác động điều kiện ổn định khi thử, thực hiện thử nghiệm về chức năng.

2.2.2.3 Tình trạng của mẫu thử trong điều kiện ổn định khi thử

Lắp mẫu thử theo quy định trong 9.2.1.2.2 và nối với nguồn cấp điện thích hợp, theo dõi và cấp điện vào mẫu (xem 9.2.1.2.3).

Mẫu thử phải ở trạng thái tĩnh lặng.

2.2.2.4 Điều kiện ổn định khi thử

Tác động điều kiện ổn định khi thử sau:

- Nhiệt độ: 55 °C ± 2 °C;
- Độ ẩm tương đối: $93\%\ ^{+2}_{-3}\%$
- Thời gian: 4 d.

Mẫu thử phải được đặt trước vào môi trường có điều kiện nhiệt độ ổn định ở mức (55 ± 2) ^{0}C cho đến khi đạt đến trạng thái ổn định nhiệt để tránh việc nước ngưng đọng thành giọt bên trên mẫu.

2.2.2.5 Các phép đo trong quá trình chịu tác động của điều kiện ổn định khi thử

Theo dõi mẫu thử trong suốt khoảng thời gian chịu tác động của điều kiện ổn định khi thử để phát hiện mọi thay đổi về tình trạng. Trong một giờ cuối của thời gian tác động của điều kiện ổn định khi thử, thực hiện thử nghiệm về chức năng của mẫu.

2.2.2.6 Các phép đo cuối

Sau khoảng thời gian để hồi phục, thực hiện thử nghiệm về chức năng của mẫu và kiểm tra mẫu bằng trực quan để phát hiện mọi hư hỏng về mặt cơ học ở cả bên trong và bên ngoài.

2.3 Va đập (vận hành)

2.3.1 Mục đích của phép thử

Mục đích của phép thử là để chứng minh sức kháng của thiết bị đối với các va đập cơ học trên bề mặt mà nó có thể vẫn đảm bảo tồn tại được trong môi trường làm việc bình thường và đó là những tác động sẽ phải chịu theo dự kiến.

2.3.2 Quy trình thử nghiệm

2.3.2.1 Tổng quát

Sử dụng thiết bị và quy trình thử nghiệm theo mô tả trong TCVN 7699-2-75 (IEC 60068-2-75).

2.3.2.2 Các phép đo ban đầu

Trước khi tác động điều kiện ổn định khi thử, thực hiện thử nghiệm về chức năng.

2.3.2.3 Tình trạng của mẫu thử trong điều kiện ổn định khi thử

Lắp mẫu thử theo quy định trong 9.2.1.2.3 và nối với nguồn cấp điện thích hợp, theo dõi và cấp điện vào mẫu (xem 9.2.1.2.3).

Mẫu thử phải ở trạng thái tĩnh lặng.

2.3.2.4 Điều kiện ổn định khi thử

Tác động va đập lên tất cả các bề mặt có thể tiếp cận được ở mức truy cập 1 của mẫu.

Với mỗi bề mặt như vậy, tác động 3 va đập lên các điểm bất kì được xem là dễ gây ra hư hại cho mẫu hoặc làm hỏng sự vận hành của mẫu.

Cần phải cẩn thận để đảm bảo rằng các kết quả từ mỗi đợt 3 lần va đập không ảnh hưởng đến những đợt va đập tiếp sau đó.

Nếu có nghi ngờ đối với một khuyết tật, thì phải loại bỏ khuyết tật đó và thực hiện một đợt 3 va đập khác lên đúng vị trí đó trên một mẫu thử khác.

Tác động điều kiện ổn định khi thử sau:

- Năng lượng va đập: (0,5 ± 0,04) J;

- Số lần va đập trên 1 điểm 3.

2.3.2.5 Các phép đo trong quá trình chịu tác động của điều kiện ổn định khi thử

Theo dõi mẫu thử trong suốt khoảng thời gian chịu tác động của điều kiện ổn định khi thử để phát hiện mọi thay đổi về trạng thái chức năng và để đảm bảo rằng các kết quả của 3 va đập không ảnh hưởng đến những đợt va đập tiếp theo.

2.3.2.6 Các phép đo cuối

Sau khi tác động điều kiện ổn định khi thử, thực hiện thử nghiệm về chức năng của mẫu và kiểm tra mẫu

bằng trực quan để phát hiện mọi hư hỏng về mặt cơ học ở cả bên trong và bên ngoài.

2.4 Rung, dao động hình sin (vận hành)

2.4.1 Mục đích của phép thử

Mục đích của phép thử là để chứng minh sức kháng của thiết bị đối với các hiện tượng rung ở mức độ phù hợp với môi trường làm việc.

2.4.2 Quy trình thử nghiệm

2.4.2.1 Tổng quát

Sử dụng quy trình thử nghiệm theo mô tả trong TCVN 7699-2-6 (IEC 60068-2-6).

Có thể kết hợp thử nghiệm vận hành chịu rung với thử nghiệm độ bền chịu rung, do vậy mẫu thử chịu tác động của điều kiện ổn định khi thử vận hành rồi sau đó chịu tác động của điều kiện ổn định khi thử độ bền theo từng hướng trục.

2.4.2.2 Các phép đo ban đầu

Trước khi cho tác động của của điều kiện ổn định khi thử, thực hiện thử nghiệm về chức năng của mẫu.

2.4.2.3 Tình trạng của mẫu thử trong điều kiện ổn định khi thử

Lắp mẫu thử theo quy định trong 9.2.1.2.2 và phù hợp với TCVN 7699-2-47 (IEC 60068-2-47) và nối với nguồn cấp điện thích hợp, theo dõi và cấp điện vào mẫu (xem 9.2.1.2.3).

Tiến hành thử đối với mẫu trong từng trạng thái chức năng sau

a) trạng thái tĩnh lặng:

b) trạng thái báo động cháy, kích hoạt ở một vùng;

c) trạng thái tắt, kích hoạt bởi lệnh tắt của một vùng và một đầu ra phù hợp với ISO 7240-1.

2.4.2.4 Điều kiện ổn định khi thử

Cho mẫu thử chịu tác động rung theo từng hướng của một nhóm 3 hướng trục lần lượt vuông góc với nhau, trong đó có một trục vuông góc với bề mặt lắp đặt mẫu.

Tác động điều kiện ổn định khi thử sau:

- Dải tần số: 10 Hz đến 150 Hz;
- Độ lớn của gia tốc: 0,981 m/s^2 (0,1 g_n);
- Số hướng trục: 3;
- Số lượng chu kỳ theo mỗi trục: 1 cho mỗi một trạng thái chức năng

2.4.2.5 Các phép đo trong quá trình chịu tác động của điều kiện ổn định khi thử

Theo dõi mẫu thử trong suốt khoảng thời gian chịu tác động của điều kiện ổn định khi thử để phát hiện

mọi thay đổi về trạng thái chức năng.

2.4.2.6 Các phép đo cuối

Sau khi chịu tác động của điều kiện ổn định khi thử, thực hiện thử nghiệm về chức năng của mẫu và kiểm tra mẫu bằng trực quan để phát hiện mọi hư hỏng về mặt cơ học ở cả bên trong và bên ngoài.

2.5 Tính tương thích điện tử (EMC), thử kháng nhiễm (vận hành)

2.5.1 Thực hiện các phép thử tính tương thích điện tử (EMC), thử kháng nhiễm sau theo quy định trong EN 50130-4

a) Sự thay đổi của hiệu điện thế nguồn cấp điện: các thử nghiệm này được đưa vào vì chúng cần được tác động vào thiết bị cấp nguồn điện được đặt trong SPT (TCVN 7568-4 (ISO 7240-4)) hoặc nếu SPT có bao gồm cả đầu vào nguồn điện mà các phép thử này áp dụng được cho những đầu vào đó;

b) Sự sụt và gián đoạn hiệu điện thế nguồn cấp điện: Các thử nghiệm này được đưa vào vì chúng cần được tác động vào thiết bị cấp nguồn điện được đặt trong SPT (TCVN 7568-4 (ISO 7240-4)) hoặc nếu SPT có bao gồm cả đầu vào nguồn điện mà các phép thử này áp dụng được cho những đầu vào đó;

c) Phóng tĩnh điện;

d) Trường điện tử bức xạ;

e) Các rối loạn bị lan truyền gây ra bởi trường điện từ;

f) Nổ nhanh dòng tức thời;

g) Sốc chậm do điện thế năng lượng cao;

2.5.2 Đối với các phép thử trong 2.5.1, phải áp dụng các tiêu chí phù hợp quy định trong EN 50130-4 và những tiêu chí sau:

a) Thử nghiệm về chức năng được đưa ra đối với các phép đo ban đầu và các phép đo cuối phải là các thử nghiệm chức năng được mô tả trong 9.2.2

b) Trạng thái vận hành được yêu cầu phải là trạng thái được quy định trong 9.2.1.2.3 và thiết bị phải được thử nghiệm ở trạng thái tĩnh lặng.

c) Các dây nối với những đầu ra và đầu vào khác nhau phải là cáp không có vỏ chống nhiễu, trừ trường hợp các thông số lắp đặt của nhà sản xuất quy định rằng phải sử dụng cáp có vỏ chống nhiễu.

d) Trong thử nghiệm phóng tĩnh điện, máy phóng phải được đặt vào các phần của thiết bị có thể truy cập được ở mức truy cập 2.

e) Trong thử nghiệm nổ nhanh dòng tức thời, các dòng tức thời phải được đặt lên dây nối với nguồn điện A.C. bằng phương pháp truyền trực tiếp và đặt lên các đầu vào khác, dây dẫn tín hiệu, dữ liệu và kiểm soát bằng phương pháp kẹp tụ (kẹp điện dung).

f) Nếu thiết bị có nhiều dạng đầu vào và đầu ra khác biệt, thì phải áp dụng các thử nghiệm theo 2.5.1 e),

f) và g) và nếu thích hợp thì cả a) và b) cho từng dạng một.

2.6 Sự biến đổi của điện thế nguồn cấp (vận hành)

2.6.1 Mục đích của phép thử

Mục đích của phép thử là để chứng minh khả năng đảm bảo chức năng làm việc đúng trong điều kiện chịu một dải hiệu điện thế dự kiến trước.

2.6.2 Quy trình thử nghiệm

2.6.2.1 Tổng quát

Hiện nay chưa thể tham chiếu đến tiêu chuẩn quốc tế được chấp nhận khác.

Cho mẫu thử chịu tác động của từng điều kiện nguồn cấp điện cho đến khi đạt đến sự ổn định nhiệt độ và thực hiện xong thử nghiệm về chức năng.

2.6.2.2 Các phép đo ban đầu

Trước khi cho tác động của điều kiện ổn định khi thử, thực hiện thử nghiệm về chức năng của mẫu.

2.6.2.3 Tình trạng của mẫu thử trong điều kiện ổn định khi thử

Lắp mẫu thử theo quy định trong 9.2.1.2.2 và nối với nguồn cấp điện thích hợp, theo dõi và cấp điện vào mẫu (xem 9.2.1.2.3).

Mẫu thử phải được thử nghiệm ở trạng thái tĩnh lặng.

2.6.2.4 Điều kiện ổn định khi thử

Tác động điều kiện ổn định khi thử sau:

a) Hiệu điện thế đầu vào lớn nhất được quy định bởi nhà sản xuất;

b) Hiệu điện thế đầu vào nhỏ nhất được quy định bởi nhà sản xuất.

Ghi chú: Tính tương thích giữa SPT với bất kỳ dạng thiết bị nguồn cấp điện cụ thể nào đòi hỏi dải hiệu điện thế đầu vào được quy định cho SPT phải bao được cả dải hiệu điện thế đầu ra được ghi nhận đối với thiết bị cấp nguồn trong các thử nghiệm của TCVN 7568-4 (ISO 7240-4).

2.6.2.5 Các phép đo trong quá trình chịu tác động của điều kiện ổn định khi thử

Theo dõi mẫu thử ngay khi chịu các điều kiện về hiệu điện thế cho đến khi đạt đến trạng thái ổn định nhiệt rồi cho mẫu thử chịu tác động của thử nghiệm về chức năng ở từng điều kiện hiệu điện thế.

2.6.2.6 Các phép đo cuối

Sau khi tác động của điều kiện ổn định khi thử, thực hiện thử nghiệm về chức năng của mẫu.

2.7 Điều kiện ẩm nhiệt, trạng thái ổn định (độ bền)

2.7.1 Mục đích của phép thử

Mục đích của phép thử là để chứng minh khả năng thiết bị chịu được những tác động dài hạn của độ ẩm trong môi trường làm việc (ví dụ như thay đổi về các đặc trưng điện học do sự hấp thụ, các phản ứng hóa học liên quan đến tình trạng ẩm, ăn mòn điện hóa, v.v.).

2.7.2 Quy trình thử nghiệm

2.7.2.1 Tổng quát

Sử dụng quy trình thử nghiệm theo mô tả trong TCVN 7699-2-78 (IEC 60068-2-78).

2.7.2.2 Các phép đo ban đầu

Trước khi cho tác động của điều kiện ổn định khi thử, thực hiện thử nghiệm về chức năng của mẫu.

2.7.2.3 Tình trạng của mẫu thử trong điều kiện ổn định khi thử

Lắp mẫu thử theo quy định trong 9.2.1.2.2 và nối với nguồn cấp điện thích hợp, theo dõi và cấp điện vào mẫu (xem 9.2.1.2.3). Trong suốt quá trình chịu tác động của điều kiện ổn định khi thử không được nối nguồn điện vào mẫu.

2.7.2.4 Điều kiện ổn định khi thử

Tác động điều kiện ổn định khi thử sau:

- Nhiệt độ: (40 ± 2) °C;
- Độ ẩm tương đối: $93\%\ ^{+2}_{-3}\%$
- Thời gian: 21 d.

Mẫu thử phải được đặt trước vào môi trường có điều kiện nhiệt độ ổn định ở mức (40 °C ± 2 °C) cho đến khi đạt đến trạng thái ổn định nhiệt để tránh việc nước ngưng đọng thành giọt bên trên mẫu.

2.7.2.5 Các phép đo cuối

Sau khoảng thời gian để hồi phục, thực hiện thử nghiệm về chức năng của mẫu và kiểm tra mẫu bằng trực quan để phát hiện mọi hư hỏng về mặt cơ học ở cả bên trong và bên ngoài.

2.8 Rung, dao động hình sin (độ bền)

2.8.1 Mục đích của thử nghiệm

Mục đích của phép thử là để chứng minh khả năng của thiết bị chịu được các ảnh hưởng dài hạn của các hiện tượng rung ở mức độ phù hợp với môi trường làm việc.

2.8.2 Quy trình thử nghiệm

2.8.2.1 Tổng quát

Sử dụng quy trình thử nghiệm theo mô tả trong TCVN 7699-2-6 (IEC 60068-2-6).

Có thể kết hợp thử nghiệm độ bền chịu rung với thử nghiệm vận hành chịu rung, do vậy mẫu thử chịu tác động của điều kiện ổn định khi thử nghiệm vận hành rồi sau đó chịu tác động của điều kiện ổn định

khi thử độ bền lần lượt theo từng hướng trục.

2.8.2.2 Các phép đo ban đầu

Trước khi cho tác động của điều kiện ổn định khi thử, thực hiện thử nghiệm về chức năng của mẫu.

2.8.2.3 Tình trạng của mẫu thử trong điều kiện ổn định khi thử

Lắp mẫu thử theo quy định trong 9.2.1.2.2 và phù hợp với TCVN 7699-2-47 (IEC 60068-2-47) và nối với nguồn cấp điện thích hợp, theo dõi và cấp điện vào mẫu (xem 9.2.1.2.3). Không được cấp nguồn điện cho mẫu trong suốt thời gian chịu tác động của điều kiện ổn định khi thử.

2.8.2.4 Điều kiện ổn định khi thử

Cho mẫu thử chịu tác động rung theo từng hướng của một nhóm 3 hướng trục lần lượt vuông góc với nhau, trong đó có một trục vuông góc với bề mặt lắp đặt mẫu.

Tác động điều kiện ổn định khi thử sau:

- Dải tần số: 10 Hz đến 150 Hz;

- Độ lớn của gia tốc: 4,905 m/s^2 (0,5 g_n);

- Số hướng trục: 3;

- Số lượng chu kỳ theo mỗi trục: 20 cho mỗi một trạng thái chức năng

2.8.2.5 Các phép đo cuối

Sau khi cho tác động của điều kiện ổn định khi thử, thực hiện thử nghiệm về chức năng của mẫu và kiểm tra mẫu bằng trực quan để phát hiện mọi hư hỏng về mặt cơ học ở cả bên trong và bên ngoài.

2.9 Báo cáo thử nghiệm

Báo cáo thử nghiệm ít nhất phải bao gồm những thông tin sau:

a) Nhận dạng về mẫu thử;

b) Viện dẫn đến tiêu chuẩn này

c) Các kết quả thử nghiệm: thời gian kích hoạt riêng và tất cả các dữ liệu, ví dụ như chiều lắp đặt mẫu, theo như chỉ định trong từng phép thử nghiệm:

d) Thời gian tác động của điều kiện môi trường và điều kiện không khí khi tác động điều kiện môi trường:

e) Nhiệt độ và độ ẩm tương đối trong phòng thử nghiệm trong suốt quá trình thử;

f) Chi tiết về thiết bị cấp và kiểm soát nguồn điện và các tiêu chí về sự kích hoạt;

g) Chi tiết về mọi sai khác so với tiêu chuẩn này hoặc so với các tiêu chuẩn ISO khác được viện dẫn, và chi tiết của tất cả các chế độ vận hành được coi là tùy chọn.

Phụ lục E

(quy định)

Chương trình thử nghiệm chức năng của RCT

1 Mức truy cập

1.1 Mục đích của thử nghiệm:

Để chứng minh khả năng của RCT theo quy định tại 7.2 đối với 4 mức truy cập và xác minh các chức năng và điều khiển được truy cập đúng theo mức truy cập cho phép.

1.2 Nguyên tắc

Bài kiểm tra bao gồm việc sử dụng các chức năng và điều khiển theo yêu cầu của 7.2, vận hành RCT ở mỗi mức truy cập và xác minh rằng quyền truy cập được cấp cho các chức năng được phép và bị từ chối truy cập vào các chức năng không được phép. Trình tự, nội dung bài kiểm tra được trình bày tại Bảng E.1

Bảng E.1. Kiểm tra mức truy cập

Bước	Điều kiện kiểm tra	Quy trình kiểm tra	Đo lường/ ghi nhận	Tiêu chí đạt
1	RCT và các thiết bị cần thiết được cài đặt và hoạt động.	Tại mức truy cập 1, thử vận hành tất cả các chức năng và điều khiển của cấp 1.	Ghi nhận xem quyền truy cập có được cho phép không.	Quyền truy cập đúng theo quy định tại mục 7.2 và phụ lục C
2	Như trên	Lặp lại bước 1 cho mức truy cập 2.	Như trên	Như trên
3	Như trên	Lặp lại bước 1 cho mức truy cập 3.	Như trên	Như trên
4	Như trên	Lặp lại bước 1 cho mức truy cập 4.	Ghi nhận xem mức 4 chỉ truy cập được nếu được cấp quyền bởi người dùng cấp 3.	Như trên
5	Như trên	Thử truy cập bằng cách nhập sai khóa truy cập 3 lần.	Ghi nhận xem quyền truy cập bị từ chối hay không.	Không được phép truy cập.
6	Sau bước 5	Chờ dưới 300 giây, thử lại với khóa hợp lệ.	Ghi nhận xem quyền truy cập có bị từ chối không.	Không được phép truy cập.
7	Sau bước 5	Chờ thời gian lâu hơn quy định của nhà sản xuất, thử lại với khóa hợp lệ.	Ghi nhận xem quyền truy cập có được phép hay không.	Quyền truy cập được phép.

Bảng E.1 (tiếp tục)

Bước	Điều kiện kiểm tra	Quy trình kiểm tra	Đo lường/ ghi nhận	Tiêu chí đạt
8	Như trên	Giữ nguyên khóa mặc định của nhà sản xuất.	Ghi nhận xem việc hoàn tất cài đặt có bị ngăn cản nếu không thay đổi khóa gốc (của nhà máy) hay không.	khóa phải được thay đổi, nếu không cài đặt sẽ không thể hoàn thành.
9	Xem bằng chứng của nhà sản xuất về chất lượng của thuật toán được sử dụng để đạt được quyền truy cập từ xa với khóa có ít nhất 1000 000 khác biệt.	Xem tài liệu xác minh thuật toán chất lượng do nhà sản xuất cung cấp.	-	Tài liệu phải nêu rõ thuật toán hỗ trợ phân biệt ít nhất 1.000.000 mã khóa khác nhau.

2 Tải lên và tải xuống phần mềm

2.1 Mục đích thử nghiệm

Nguyên tắc của thử nghiệm này là để chứng minh rằng việc tải lên và tải xuống phần mềm của RCT, nếu được triển khai, tuân thủ các yêu cầu của 7.3.

2.2 Nguyên tắc

Bài kiểm tra bao gồm việc cố gắng cập nhật phần mềm của RCT, vận hành RCT ở mức truy cập phù hợp và làm theo hướng dẫn trong sổ tay hướng dẫn RCT.

Bảng E.2. Kiểm tra tải lên và tải xuống phần mềm

Bước	Điều kiện kiểm tra	Quy trình kiểm tra	Đo lường	Tiêu chí đạt
1	RCT và các thiết bị cần thiết được cài đặt và hoạt động	Ở mức truy cập 1, thử cập nhật phần mềm.	Ghi nhận xem việc cập nhật phần mềm có được phép hay không.	Không được phép cập nhật phần mềm.
2	Như trên	Lặp lại như bước 1 cho mức truy cập 2.	Như trên	Như trên
3	Như trên	Lặp lại như bước 1 cho mức truy cập 3.	Như trên	Như trên
4	Như trên	Thử cập nhật phần mềm ở mức truy cập 4.	Như trên	Được phép cập nhật phần mềm.
5	Như trên	Ngắt kết nối mạng trong khi thực hiện cập nhật phần mềm.	Ghi nhận xem RCT có tiếp tục hoạt động bình thường hay không.	RCT phải hoạt động bình thường sau khi cố gắng tải xuống phần mềm

3 Lưu trữ tham số

3.1 Mục tiêu kiểm tra:

Chứng minh rằng RCT đáp ứng mục 7.4, có khả năng bảo vệ dữ liệu lưu trữ (tham số và dữ liệu khách hàng) trước các sự cố mất nguồn hoặc khởi động lại.

3.2 Nguyên tắc:

Thay đổi ít nhất 2 tham số đặc thù tại của địa điểm, sau đó kiểm tra lại các tham số này sau khi mất nguồn/ phục hồi nguồn hoặc khởi động lại thiết bị.

Bảng E.3. Kiểm tra lưu trữ tham số

Bước	Điều kiện kiểm tra	Quy trình kiểm tra	Đo lường	Tiêu chí đạt
1	RCT và các thiết bị cần thiết đã được cài đặt và hoạt động.	Thay đổi và lưu ít nhất 2 tham số đặc thù của địa điểm theo hướng dẫn.	Ghi nhận xem các thay đổi có được lưu lại hay không.	-
2	Như trên	Tắt nguồn thiết bị.	-	-
3	RCT ở trạng thái tắt nguồn.	Chờ ít nhất 10 giây và bật nguồn lại.	Ghi nhận xem RCT có quay lại trạng thái hoạt động bình thường không.	RCT phải hoạt động bình thường sau khi khởi động lại như trước khi tắt nguồn
4	Như bước 1	Đọc lại các tham số đã thay đổi theo hướng dẫn.	Ghi nhận giá trị các tham số.	Giá trị tham số phải khớp với trước khi mất nguồn.
5	Như trên	Lặp lại bước 2-4 theo quy trình khởi động lại được quy định.	Ghi nhận giá trị các tham số.	Giá trị tham số không thay đổi sau khởi động lại.

4 Giám sát và thông báo lỗi ATS cho đường truyền kép

4.1 Mục tiêu kiểm tra:

Chứng minh rằng RCT thông báo lỗi ATS đến AMS như quy định tại 5.3.3.4

4.2 Nguyên tắc:

Cấu hình SPT để phù hợp với thời gian báo cáo của từng loại đường truyền kép được hỗ trợ bởi RCT. Kết nối SPT với RCT qua hai mạng truyền dẫn sử dụng công nghệ khác nhau, sau đó vô hiệu hóa SPT và ghi nhận rằng lỗi ATS được thông báo tới AMS trong thời gian báo cáo tối đa cho phép.

4.3 Điều kiện kiểm tra:

SPT ở trạng thái hoạt động hoàn toàn, được kết nối với RCT qua hai mạng truyền dẫn khác nhau.

4.4 Quy trình kiểm tra:

Vô hiệu hóa SPT bằng cách tắt nguồn của nó.

4.5 Đo lường:

Ghi nhận tín hiệu lỗi ATS được truyền tới AMS.

4.6 Tiêu chí đạt:

Lỗi ATS phải được truyền tới AMS trong thời gian báo cáo tối đa cho phép.

Tùy chọn: Lỗi ATP cũng có thể được truyền tới AMS.

5 Giao diện tới AMS

5.1 Mục tiêu kiểm tra:

Chứng minh rằng giao diện giữa RCT và AMS tuân thủ các yêu cầu tại mục 7.6.

5.2 Nguyên tắc:

Thực hiện cấu hình RCT và kết nối với AMS theo hướng dẫn của nhà sản xuất.

Bảng E.4: Kiểm tra giao diện tới AMS

Bước	Điều kiện kiểm tra	Quy trình kiểm tra	Đo lường	Tiêu chí đạt
1	RCT và các thiết bị cần thiết đã được cài đặt và hoạt động.	Kết nối RCT với AMS theo tài liệu hướng dẫn.	Ghi nhận xem kết nối có tuân thủ tài liệu hay không.	Giao diện giữa AMS và RCT phải hoạt động.
2	Như trên	Ngắt kết nối giao diện AMS.	Ghi nhận thời gian cho đến khi lỗi AMS được thông báo tại RCT.	Thời gian thông báo phải phù hợp với các yêu cầu tại mục 7.6.

6 Tín hiệu lỗi

6.1 Mục tiêu kiểm tra:

Mục tiêu của bài kiểm tra này là chứng minh rằng tín hiệu lỗi từ RCT tuân thủ các yêu cầu tại mục 7.7.

6.2 Nguyên tắc:

Thực hiện các bài kiểm tra gây ra lỗi và theo dõi xem các lỗi có được RCT thông báo tới AMS hay không.

Bảng E.5: Kiểm tra tín hiệu lỗi

Bước	Điều kiện kiểm tra	Quy trình kiểm tra	Đo lường	Tiêu chí đạt
1	Điều kiện chung: RCT kết nối với AMS.	Kích hoạt lỗi trên hệ thống ATS.	Theo dõi xem lỗi ATS có được thông báo đến AMS không.	Lỗi ATS phải được thông báo tới AMS.
2	Như trên	Kiểm tra nếu báo cáo lỗi ATP được triển khai.	Kích hoạt lỗi ATP.	Lỗi ATP phải được thông báo tới AMS.
3	Như trên	Kích hoạt lỗi giao diện AMS.	Theo dõi xem lỗi AMS có được ghi nhận hay không.	Lỗi AMS phải được ghi nhận theo tài liệu của nhà sản xuất.
4	Như trên	Kích hoạt lỗi giao diện mạng truyền dẫn.	Theo dõi xem lỗi giao diện mạng có được thông báo đến AMS không.	Lỗi giao diện mạng phải được thông báo theo tài liệu của nhà sản xuất.
5	(Tùy chọn, chỉ trong trường hợp RCT được lưu trữ)	Kích hoạt lỗi giao diện mạng truyền dẫn giữa RCT-H và RCT-A	Theo dõi xem lỗi giao diện mạng có được thông báo đến AMS và ATSP không.	Lỗi giao diện mạng phải được thông báo và nếu gây ra lỗi ATS, lỗi ATS phải được thông báo đến AMS và ATSP.

7 Xử lý tín hiệu báo động

7.1 Mục tiêu kiểm tra:

Mục tiêu của bài kiểm tra này là chứng minh khả năng của RCT trong việc nhận, xử lý và chuyển tiếp tín hiệu hoặc thông điệp từ ATS.

7.2 Nguyên tắc:

Bài kiểm tra này gồm việc xác minh xem tín hiệu báo động hoặc thông điệp được gửi đến giao diện mạng truyền dẫn của RCT có được nhận và xử lý chính xác, sau đó chuyển tiếp đến AMS hay không.

7.3 Điều kiện kiểm tra:

RCT được lắp đặt và cài đặt theo hướng dẫn của nhà sản xuất. Nếu có nhiều giao diện mạng truyền dẫn cho ATS, bài kiểm tra phải được thực hiện cho từng giao diện.

7.4 Quy trình kiểm tra:

Tạo tín hiệu báo động hoặc thông điệp trên giao diện mạng truyền dẫn của RCT.

7.5 Đo lường:

Ghi nhận việc tiếp nhận tín hiệu báo động hoặc thông điệp.

7.6 Tiêu chí đạt:

Tín hiệu báo động hoặc thông điệp phải được tiếp nhận và chuyển tiếp tới AMS.

8 Ghi lại sự kiện:

8.1 Mục tiêu kiểm tra:

Mục tiêu của bài kiểm tra này là chứng minh rằng RCT ghi lại tất cả các sự kiện đã thực hiện và bảo vệ chúng khỏi sự cố mất nguồn, như yêu cầu tại mục 7.8.

8.2 Nguyên tắc:

Bài kiểm tra này bao gồm việc kích hoạt tất cả các chức năng đã được thực hiện và tạo ra tất cả các sự kiện yêu cầu trong Bảng 4, sau đó kiểm tra chúng có được ghi lại trong nhật ký sự kiện của **RCT** và bảo vệ khỏi sự cố mất điện hay không.

Bảng E.6: Kiểm tra ghi lại sự kiện

Bước	Điều kiện kiểm tra	Quy trình kiểm tra	Đo lường	Tiêu chí đạt
1	RCT và các thiết bị cần thiết đã được cài đặt và hoạt động.	Tạo tất cả sự kiện theo yêu cầu trong Bảng 4 ít nhất một lần.	Kiểm tra xem tất cả các sự kiện có được ghi lại đúng cách không.	Tất cả các sự kiện phải được ghi lại chính xác, với dấu thời gian.
2	Như trên	Ngắt nguồn và khôi phục lại nguồn cho RCT.	Kiểm tra xem các sự kiện có bị ảnh hưởng không.	Các sự kiện phải vẫn được ghi lại chính xác sau khi mất nguồn.

9 Độ phân giải thời gian và đồng bộ hóa:

9.1 Mục tiêu kiểm tra:

Mục tiêu của bài kiểm tra này là chứng minh rằng độ chính xác của dấu thời gian (timestamps) đính kèm với các sự kiện trong nhật ký đáp ứng yêu cầu tại mục 7.8.

9.2 Nguyên tắc:

Bài kiểm tra này bao gồm việc tạo ra các sự kiện và kiểm tra dấu thời gian của chúng so với nguồn thời gian tham chiếu.

Các bài kiểm tra phải được thực hiện so với một nguồn thời gian tham chiếu đã được xác định rõ ràng. Một máy chủ NTP (Network Time Protocol) cấp độ Stratum 2 (thường có sẵn trên Internet) có thể được sử dụng để cung cấp độ chính xác yêu cầu.

Bảng E.7: Kiểm tra độ phân giải đồng hồ và đồng bộ hóa

Bước	Điều kiện kiểm tra	Quy trình kiểm tra	Đo lường	Tiêu chí đạt
1	Trạng thái đã được cài đặt và hoạt động bình thường.	Đồng bộ đồng hồ theo thông số kỹ thuật của nhà sản xuất.	Ghi nhận xem thời gian có được đồng bộ với UTC hay không.	Thời gian phải được đồng bộ với UTC.
2	Trạng thái đã được cài đặt và hoạt động bình thường.	Tạo sự kiện.	Ghi lại dấu thời gian khi tạo sự kiện.	Phải có một mục nhật ký với độ phân giải ít nhất là 1 giây và sai lệch so với thời gian tham chiếu dưới 5 giây.
3	Sau bước 2	Chờ ít nhất 72 giờ và tạo sự kiện thứ hai.	Ghi lại dấu thời gian của sự kiện thứ hai.	Như trên, phải có dấu thời gian chính xác.

10 Độ bền của nhật ký:

Xác minh tài liệu của nhà sản xuất về cách đảm bảo rằng các mục nhật ký có **tuổi thọ 3 năm**.

11 Phương pháp tối ưu hóa lưu trữ sự kiện

11.1 Mục tiêu kiểm tra

Nếu việc tối ưu hóa lưu trữ sự kiện bằng cách nhóm các sự kiện lại như mô tả trong mục 7.8 được triển khai, cần kiểm tra việc nhóm và đóng dấu thời gian.

11.2 Nguyên tắc

Bài kiểm tra này bao gồm việc tạo ra các sự kiện lặp lại liên tục giống nhau và kiểm tra xem chúng có được ghi lại trong RCT theo yêu cầu tại 7.8 hay không.

Bảng E.8: Kiểm tra tối ưu hóa nhật ký

Bước	Điều kiện kiểm tra	Quy trình kiểm tra	Đo lường	Tiêu chí đạt
1	**RCT** và các thiết bị cần thiết đã được cài đặt và hoạt động.	Tạo ra các sự kiện giống hệt nhau và lặp lại.	Kiểm tra xem các sự kiện có được ghi lại đúng cách không.	Tất cả các sự kiện phải được ghi lại đúng cách, với dấu thời gian và số lượng sự kiện giống nhau.

12 Nhận dạng người dùng cho các mục nhật ký

12.1 Mục tiêu kiểm tra

Xác minh rằng nhận dạng người dùng cho các mục nhật ký như thay đổi cấu hình, thay đổi người dùng hoặc quyền truy cập, thay đổi thủ công thời gian và ngày tháng, thay đổi phần mềm và truy cập vào RCT, đều được ghi lại.

12.2 Nguyên tắc:

Bài kiểm tra này bao gồm việc tạo ra các mục nhật ký sau:

- Thay đổi cấu hình, thay đổi người dùng và quyền truy cập.

- Thay đổi thủ công thời gian và ngày tháng.

- Thay đổi phần mềm và quyền truy cập vào RCT.

- Kiểm tra xem các mục này có được ghi lại với nhận dạng người dùng hay không.

Bảng E.9: Kiểm tra nhật ký nhận dạng người dùng

Bước	Điều kiện kiểm tra	Quy trình kiểm tra	Đo lường	Tiêu chí đạt
1	**RCT** và các thiết bị cần thiết đã được cài đặt và hoạt động.	Tạo ít nhất một mục nhật ký cho các thay đổi cấu hình, thay đổi người dùng, thay đổi phần mềm, v.v.	Kiểm tra xem các sự kiện có được ghi lại với nhận dạng người dùng không.	Tất cả các mục nhật ký phải được ghi lại cùng với nhận dạng người dùng.

13 Chế độ vận hành

13.1 Mục tiêu kiểm tra:

Tài liệu của nhà sản xuất phải cung cấp thông tin về các chế độ vận hành mà hệ thống hỗ trợ.

13.2 Mục tiêu kiểm tra:

Chứng minh rằng tất cả các chế độ vận hành được hỗ trợ đều tuân thủ các yêu cầu tại mục 7.9.

13.3 Nguyên tắc:

Thực hiện kích hoạt báo động từ FDAD và/hoặc SPT tới RCT(s), và theo dõi xem RCT(s) có truyền lại thông báo xác nhận từ RCT đến SPT và/hoặc FDAD trong các điều kiện giao diện AMS khác nhau hay không.

Bảng E.10: Kiểm tra chế độ vận hành

Bước	Điều kiện kiểm tra	Quy trình kiểm tra	Đo lường	Tiêu chí đạt
1	Trạng thái chung: RCT được kết nối với AMS.	Kích hoạt báo động từ FDAD/SPT tới RCT(s).	Theo dõi xem báo động có được hiển thị tại AMS(s) trong thời gian yêu cầu của ATS.	Báo động phải hiển thị tại AMS(s).
2	Trạng thái chung, và không có AMS(s) được kết nối.	Kích hoạt báo động từ FDAD/SPT tới RCT(s).	Theo dõi xem báo động có hiển thị tại AMS không.	Không có báo động hiển thị tại AMS(s).
3	Như sau bước 2, chờ ít nhất thời gian truyền tải yêu cầu của ATS.	Khôi phục giao diện AMS (tức là kết nối lại RCT(s) với AMS(s)).	Theo dõi xem báo động đã kích hoạt trong bước 2 có được hiển thị tại AMS(s) không.	Báo động phải hiển thị tại AMS(s).

14 Tấn công từ chối dịch vụ

14.1 Mục tiêu kiểm tra:

Mục tiêu của bài kiểm tra này là xác định rằng tài liệu của nhà sản xuất nêu rõ rằng tấn công từ chối dịch vụ (DoS) trên một giao diện mạng truyền dẫn không làm ảnh hưởng đến hoạt động của RCT hoặc hoạt động của bất kỳ giao diện truyền dẫn mạng nào khác của RCT.

14.2 Nguyên tắc:

Bài kiểm tra này bao gồm việc kiểm tra tài liệu của nhà sản xuất liên quan đến RCT.

14.3 Quy trình kiểm tra:

Kiểm tra tài liệu của nhà sản xuất liên quan đến RCT để xác nhận rằng tấn công từ chối dịch vụ trên một giao diện mạng truyền dẫn không làm ảnh hưởng đến hoạt động của RCT hoặc bất kỳ giao diện truyền dẫn mạng nào khác.

14.4 Đo lường

Kiểm tra tài liệu của nhà sản xuất về phần bảo vệ tấn công từ chối dịch vụ và xác nhận rằng một tấn công từ chối dịch vụ trên một giao diện không làm gián đoạn hoạt động của RCT hoặc các giao diện khác.

14.5 Tiêu chí đạt:

Kiểm tra xác nhận thành công rằng tấn công từ chối dịch vụ trên một giao diện không ảnh hưởng đến các giao diện truyền dẫn mạng khác hoặc hoạt động của RCT.

15 Bảo mật thông tin và Bảo mật chống giả mạo

15.1 Nhà sản xuất phải mô tả trong tài liệu RCT các phương pháp bảo vệ chống lại việc thay thế SPT bằng thiết bị giống hệt hoặc thiết bị giả lập theo yêu cầu tại mục 7.12.

15.2 Nhà sản xuất phải mô tả các phương pháp bảo vệ thông tin truyền qua ATS để ngăn chặn việc đọc và sửa đổi thông tin trái phép, tuân thủ các yêu cầu tại mục 7.11.

16 Dự phòng RCT

Bảng E.11: Kiểm tra dự phòng RCT

Bước	Điều kiện kiểm tra	Quy trình kiểm tra	Đo lường	Tiêu chí đạt
1	Trạng thái chung: ATS hoạt động đầy đủ và được cấu hình cho bất kỳ ATS đường dẫn kép nào. Cả hai RCT đều được kết nối với AMS.	Kích hoạt truyền báo động từ SPT tới RCT.	Theo dõi xem báo động có được nhận tại AMS không.	Báo động phải được nhận tại AMS.
2	Trạng thái chung, và: Vô hiệu hóa RCT1 (cho phép RCT2 hoạt động).	Như trên	Theo dõi xem báo động có được nhận tại AMS không.	Báo động phải được nhận tại AMS.
2b	Trạng thái chung, và: Vô hiệu hóa RCT2 (cho phép RCT1 hoạt động).	Như trên	Theo dõi xem báo động có được nhận tại AMS không.	Báo động phải được nhận tại AMS.
3	Trạng thái chung, và vô hiệu hóa tất cả các giao diện mạng truyền dẫn của cả hai RCT.	Như trên	Theo dõi xem lỗi ATS có được nhận tại AMS không.	Lỗi ATS phải được nhận tại AMS.

17 Tài liệu

Xác minh rằng tất cả các tài liệu bắt buộc đều được cung cấp đầy đủ và chính xác.

Phụ lục F

(Quy định)

Giao diện giữa FDAD và SPT

1 Giao diện song song giữa FDAD và SPT

1.1 Tổng quan

Khi giao diện song song được cung cấp, giao diện đó sẽ hoạt động như mô tả tại 1.2 và 1.3 phụ lục này. Giao diện song song tối thiểu phải cung cấp một đầu vào báo động và hai đầu ra lỗi.

1.2 Đầu vào báo động SPT song song

Việc giám sát các đầu vào SPT được thực hiện bởi SPT. Các thay đổi về giá trị điện trở cuối đường dây ± 40% trở lên sẽ dẫn đến thay đổi trạng thái nếu chúng kéo dài hơn 200 ms.

1.3 Đầu ra SPT song song

1.3.1 Tổng quan

Tất cả các đầu ra phải là tiếp điểm không có điện thế (potential free contact) hoặc bộ thu hở (open collector). Nếu đầu ra là bộ thu hở, đầu ra phải có khả năng tiêu thụ dòng điện ít nhất 20 mA.

1.3.2 Lỗi ATS

Đầu ra này phải tuân thủ các yêu cầu sau:

a) ở trạng thái bình thường (không có lỗi): đầu ra đóng (<100 Ω);

b) trong trường hợp lỗi ATS: đầu ra mở (>500 kΩ);

c) trong trường hợp lỗi SPT: đầu ra mở (>500 kΩ);

d) cài đặt theo thời gian lỗi, nhưng ít nhất là 1 giây.

2 Giao diện nối tiếp giữa FDAD và SPT

2.1 Có thể kết nối FDAD và SPT bằng bất kỳ giao diện nối tiếp và phương tiện truyền tín hiệu nào. Nếu cần bộ chuyển đổi tín hiệu, bộ định tuyến hoặc bất kỳ thiết bị hoặc hệ thống chủ động nào khác để kết nối FDAD với SPT, thiết bị hoặc hệ thống bổ sung này phải được coi là một phần của FDAD hoặc SPT, và phải bảo đảm quy định có liên quan của FDAD và SPT.

2.2 Nhà sản xuất phải chỉ định giao diện nối tiếp giữa SPT và FDAD theo Mô hình lớp 7 của ISO OSI.

2.3 Mô tả kỹ thuật giao diện phải bao gồm ít nhất các lớp vật lý, liên kết dữ liệu và ứng dụng

2.4 Giao thức nối tiếp sẽ cho phép phát hiện bất kỳ sự cố nào của kết nối trong thời gian báo cáo quy định tại tiêu chuẩn này

2.5 Nhà sản xuất sẽ cung cấp kết quả thử nghiệm và tài liệu nêu rõ khả năng tương thích với FDAD và ATS.

Thư mục tài liệu tham khảo

[1] BSEN 50136-1:2012+A1:2018 Alarm systems - Alarm transmission systems and equipment – Part 1: General requirements for alarm transmission systems;

[2] BSEN 50136-2:2013+A1:2023 Alarm systems - Alarm transmission systems and equipment – Part 2: Requirements for Supervised Premises Transceiver (SPT);

[3] BSEN 50136-3:2013+A1:2021 Alarm systems - Alarm transmission systems and equipment – Part 3: Requirements for Receiving Centre Transceiver (RCT);

[4] CLC/TS 50136-10:2022 Alarm systems - Alarm transmission systems and equipment – Part 10: Requirements for remote access.

[5] TCVN 7568-21:2016 (ISO 7240-21:2005) Hệ thống báo cháy – Phần 21: Thiết bị định tuyến;

[6] TCVN 5738:2021 Phòng cháy chữa cháy – Hệ thống báo cháy tự động – Yêu cầu kỹ thuật;

[7] EN 54-21: 2006 Fire detection and fire alarm systems - Part 21: Alarm transmission and fault warning routing equipment.