TIÊU CHUẨN QUỐC GIA

TCVN 14538 :2025

PHÒNG CHÁY CHỮA CHÁY - HỆ THỐNG TRUYỀN TIN BÁO CHÁY

Fire protection - Fire alarm transmission system

Lời nói đầu

TCVN 14538:2025 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 CHÁY

Fire protection - Fire alarm transmission system

1 Phạm vi áp dụng

1.1 Tiêu chuẩn này áp dụng đối với các hệ thống truyền tin báo cháy có chức năng tiếp nhận, truyền tải, xử lý và xác minh thông tin liên quan đến trạng thái chức năng của các thiết bị, hệ thống báo cháy trước khi chuyển tới lực lượng chữa cháy.

1.2 Tiêu chuẩn này quy định các yêu cầu kỹ thuật, tính năng hoạt động và phương pháp kiểm tra, thử nghiệm đối với hệ thống truyền tin báo cháy.

2 Tài liệu viện dẫn

Các tài liệu viện dẫn sau rất cần thiết cho việc áp dụng tiêu chuẩn này. Đối với các tài liệu viện dẫn ghi năm công bố thì áp dụng phiên bản được nêu. Đối với tài liệu viện dẫn không ghi năm công bố thì áp dụng phiên bản mới nhất, bao gồm cả các sửa đổi (nếu có).

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 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 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*

IEC 62599-2, *Alarm systems - Part 2: Electromagnetic compatibility - Immunity requirements for components of fire and security alarm systems* (Hệ thống báo động - Phần 2: Tương thích điện từ - Yêu cầu về miễn nhiễm đối với các thành phần của hệ thống báo cháy và báo động an ninh)

EN 50130-4, *Alarm systems - Part 4: Electromagnetic compatibility - Product family standard: Immunity requirements for components of fire, intruder, hold, up, CCTV, access control and social alarm systems* (Hệ thống báo động - Phần: 4: Tương thích điện từ - Tiêu chuẩn họ sản phẩm: Yêu cầu về miễn nhiễm đối với các thành phần của hệ thống báo cháy, chống trộm, báo cướp, truyền hình mạch kín (CCTV) kiểm soát ra vào và báo động xã hội)

3 Thuật ngữ, định nghĩa và chữ viết tắt

3.1 Thuật ngữ, định nghĩa

Trong tiêu chuẩn này sử dụng các thuật ngữ và định nghĩa sau:

3.1.1 Cấu trúc hệ thống truyền tin báo cháy

3.1.1.1

Hệ thống truyền tin báo cháy (fire alarm transmission system)

FATS

Hệ thống có chức năng tiếp nhận, truyền tải, xử lý và xác minh thông tin liên quan đến trạng thái của các *hệ thống báo cháy* (3.1.1.7) trước khi chuyển tới *lực lượng chữa cháy* (3.1.1.16). Hệ thống truyền tin báo cháy gồm *mạng dịch vụ truyền tin báo cháy* (3.1.1.2) và *trung tâm tiếp nhận báo cháy* (3.1.1.4).

CHÚ THÍCH: Cấu trúc của hệ thống truyền tin báo cháy được mô tả tại phụ lục A.

3.1.12

Mạng dịch vụ truyền tin báo cháy (fire alarm transmission service network)

FATSN

Tập hợp một hoặc nhiều *khối truyền tin báo cháy* (3.1.1.3) được giám sát và quản lý bởi một *đơn vị cung cấp dịch vụ truyền tin báo cháy* (3.1.1.8).

3.1.1.3

Khối truyền tin báo cháy (fire alarm transmission block)

FATB

Là một bộ phận của mạng dịch vụ truyền tin báo cháy, bao gồm thiết bị truyền tin và mạng có chức năng tiếp nhận và truyền tải thông tin liên quan đến trạng thái của một hoặc nhiều hệ thống báo cháy tại một *cơ sở được giám sát* (3.1.1.15) đến trung tâm tiếp nhận báo cháy.

CHÚ THÍCH: Cấu trúc của khối truyền tin báo cháy được mô tả tại phụ lục B.

3.1.1.4

Trung tâm tiếp nhận báo cháy (fire alarm receiving centre)

FARC

Là một bộ phận của hệ thống truyền tin báo cháy nơi có người trực liên tục, thực hiện chức năng xử lý và xác minh thông tin liên quan đến trạng thái của hệ thống báo cháy trước khi chuyển tới lực lượng chữa cháy.

3.1.1.5

Thiết bị truyền tin báo cháy (supervised premises transceiver)

SPT

Là thiết bị thuộc khối truyền tin báo cháy được lắp đặt tại cơ sở được giám sát để tiếp nhận, truyền tải thông tin liên quan đến trạng thái của hệ thống báo cháy.

3.1.1.6

Bộ phận tiếp nhận tin báo cháy (fire alarm receiving centre transceiver)

RCT

Là phần mềm hoặc thiết bị phần cứng thuộc khối truyền tin báo cháy, được lắp đặt tại trung tâm tiếp nhận báo cháy; có chức năng tiếp nhận, xử lý thông tin từ một hoặc nhiều thiết bị truyền tin báo cháy để gửi đến hệ thống quản lý tin báo cháy, đồng thời giám sát trạng thái của khối truyền tin báo cháy.

3.1.1.7

Hệ thống báo cháy (fire detection and alarm system)

FDAS

Nhóm các thành phần bao gồm thiết bị điều khiển và chỉ báo, khi được bố trí trong các cấu hình xác định, có khả năng phát hiện, chỉ báo đám cháy và đưa ra tín hiệu xử lý thích hợp

CHÚ THÍCH: Trong tiêu chuẩn này, thuật ngữ hệ thống báo cháy được hiểu theo nghĩa rộng, ngoài hệ thống báo cháy được quy định tại TCVN 7568-1, còn có thể gồm các thiết bị báo cháy độc lập hoặc thiết bị khác có khả năng phát hiện và báo cháy, có thể kết nối và truyền tin đến thiết bị truyền tin báo cháy.

3.1.1.8

Đơn vị cung cấp dịch vụ truyền tin báo cháy (fire alarm transmission service provider)

FATSP

Đơn vị chịu trách nhiệm về thiết kế, vận hành, quản lý, xác minh hiệu năng của mạng dịch vụ truyền tin báo cháy.

CHÚ THÍCH: Đơn vị cung cấp dịch vụ truyền tin báo cháy có thể đồng thời là đơn vị vận hành và quản lý trung tâm tiếp nhận báo cháy hoặc có thể ủy quyền một số trách nhiệm thông qua thỏa thuận với cơ sở được giám sát, trung tâm tiếp nhận báo cháy, nhà điều hành... nhưng phải chịu trách nhiệm tổng

thể về hoạt động của hệ thống.

3.1.1.9

Hệ thống quản lý tin báo cháy (fire alarm management system)

FAMS

Hệ thống tại trung tâm tiếp nhận báo cháy có chức năng: Tiếp nhận thông tin liên quan đến trạng thái của hệ thống báo cháy thông qua bộ phận tiếp nhận tin báo cháy; tổ chức xử lý, lưu trữ, quản lý, cho phép truy xuất dữ liệu, đồng thời tự động hiển thị các tin báo từ mỗi hệ thống báo cháy.

3.1.1.10

Đường truyền tin báo cháy (fire alarm transmission path)

FATP

Tuyến đường (route) mà một tin báo cháy hoặc báo lỗi di chuyển qua, từ một hệ thống báo cháy riêng lẻ đến hệ thống quản lý tin báo cháy có liên quan.

CHÚ THÍCH: Đường truyền tin báo cháy được bắt đầu tại giao diện giữa hệ thống báo cháy và thiết bị truyền tin báo cháy, kết thúc tại giao diện giữa bộ phận tiếp nhận tin báo cháy và hệ thống quản lý tin báo cháy. Đối với mục đích xác nhận và giám sát, hướng ngược lại cũng có thể được sử dụng.

3.1.1.11

Liên kết truyền tin (transmission link)

Một phần của mạng truyền dẫn mà một hoặc nhiều đường truyền tin báo cháy được truyền tải qua đó.

CHÚ THÍCH: Một liên kết truyền tin có thể đồng thời truyền tải các đoạn của nhiều đường truyền tin báo cháy khác nhau. Ngược lại, một đường truyền tin báo cháy cũng có thể được thiết lập bằng cách kết nối nhiều liên kết truyền tin với nhau theo cấu hình song song, nối tiếp hoặc kết hợp cả hai.

3.1.1.12

Mạng truyền dẫn (transmission network)

Mạng giữa hai hoặc nhiều thiết bị truyền tin báo cháy và bộ phận tiếp nhận tin báo cháy.

CHÚ THÍCH: Mạng truyền dẫn có thể bao gồm các thiết bị mạng 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, hệ thống dây mạng...

3.1.1.13

Bên thứ ba (third party)

Là tổ chức hoặc cá nhân cung cấp hệ thống, thiết bị hoặc ứng dụng có liên quan đến quá trình truyền tin báo cháy nhưng không phải là đơn vị cung cấp dịch vụ truyền tin báo cháy.

CHÚ THÍCH: Trong hệ thống truyền tin báo cháy, bên thứ ba có thể là các đơn vị cung cấp mạng viễn thông, các đơn vị sản xuất thiết bị định tuyến truyền tin (router, switch, mô-đun SM...).

3.1.1.14

Nhân viên trung tâm tiếp nhận báo cháy (fire alarm receiving centre operator - FARC operator)

Người trực tại trung tâm tiếp nhận báo cháy, có trách nhiệm theo dõi, đánh giá và xử lý các tin báo được hệ thống hiển thị.

3.1.1.15

Cơ sở được giám sát

Nhà, công trình hoặc địa điểm được sử dụng để ở, sản xuất, kinh doanh, làm việc hoặc mục đích khác theo quy định của pháp luật. Được trang bị hệ thống báo cháy để phát hiện nguy cơ cháy, nổ và truyền tín hiệu báo cháy đến trung tâm tiếp nhận báo cháy.

3.1.1.16

Lực lượng chữa cháy

Lực lượng có chức năng tiếp nhận tin báo cháy từ trung tâm tiếp nhận báo cháy và triển khai các biện pháp chữa cháy tại cơ sở được giám sát.

3.1.2 Trạng thái và tin báo

3.1.2.1

Báo cháy thực (genuine fire alarm)

Trạng thái của hệ thống báo cháy phản ánh tình trạng có cháy thực sự xảy ra.

3.1.2.2

Báo cháy giả (false fire alarm)

Trạng thái báo cháy của hệ thống báo cháy được gửi đến trung tâm tiếp nhận báo cháy và đã chuyển đến lực lượng chữa cháy nhưng không phải là báo cháy thực.

3.1.2.3

Chỉ báo (indication)

Là thông tin (bằng âm thanh, hình ảnh hoặc bất kỳ hình thức khác) dùng để hiển thị trạng thái của thiết bị và/hoặc hệ thống.

3.1.2.4

Lọc báo cháy (fire alarm filtering)

Quy trình trong đó các tin báo cháy được chủ động trì hoãn để xác minh trước khi chuyển đến lực lượng chữa cháy nhằm mục đích hạn chế báo cháy giả.

3.1.2.5

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

Tin báo hoặc tín hiệu được tạo ra do trạng thái lỗi của hệ thống hoặc thiết bị.

3.1.2.6

Tin báo (message)

Là một chuỗi tín hiệu được truyền đi chứa các thông tin cần thiết và được áp dụng các phương thức để đảm bảo tính toàn vẹn, khả năng chống nhiễu và khả năng tiếp nhận chính xác.

CHÚ THÍCH 1: Thông tin cần thiết có thể gồm:

- Thông tin nhận dạng giúp xác định nguồn gốc của tin báo (ví dụ từ cơ sở được giám sát, thiết bị/thành phần truyền tin nào...);

- Dữ liệu chức năng mô tả nội dung cụ thể được truyền tải, như loại tin báo (báo cháy, báo lỗi, báo thay đổi trạng thái...).

CHÚ THÍCH 2: Phương pháp đảm bảo tính toàn vẹn là phương pháp kỹ thuật được áp dụng để đảm bảo nội dung tin báo không bị thay đổi, sai lệch hoặc giả mạo trong quá trình truyền.

CHÚ THÍCH 3: Khả năng chống nhiễu là phương pháp bảo vệ tin báo khỏi các ảnh hưởng tiêu cực của nhiễu điện từ, lỗi truyền tín hiệu hoặc các tác động bên ngoài khác.

CHÚ THÍCH 4: Khả năng tiếp nhận chính xác là các phương thức kỹ thuật đảm bảo rằng tin báo được tiếp nhận đúng cách, đầy đủ và được xác nhận thành công tại điểm đích.

3.1.2.7

Trạng thái báo cháy (fire alarm condition)

Trạng thái của hệ thống báo cháy hoặc một phần của nó phản ánh mối nguy hiểm cháy.

3.1.2.8

Trạng thái lỗi (fault condition)

Trạng thái của hệ thống khi hệ thống đó hoặc một phần của nó hoạt động không bình thường.

3.1.3 Hiệu năng của hệ thống

3.1.3.1

Dung lượng hệ thống (system capacity)

Số lượng hệ thống báo cháy mà hệ thống truyền tin báo cháy có thể kết nối mà vẫn hoạt động đảm bảo quy định tại tiêu chuẩn này.

3.1.3.2

Độ khả dụng (availability, general)

Tỷ lệ phần trăm thời gian mà mạng dịch vụ truyền tin báo cháy và/hoặc các bộ phận của nó hoạt động đáp ứng yêu cầu của tiêu chuẩn này.

3.1.3.3

Thời gian báo cáo lỗi (reporting time)

Khoảng thời gian từ khi lỗi xảy ra trong khối truyền tin báo cháy cho đến khi lỗi đó được báo cáo tại bộ phận tiếp nhận tin báo cháy.

3.1.3.4

Thời gian truyền (transmission time)

Là khoảng thời gian tính từ khi một tin báo (báo cháy, báo lỗi) hoặc thay đổi trạng thái xảy ra tại hệ thống báo cháy được đưa ra để truyền tại giao diện giữa hệ thống báo cháy và thiết bị truyền tin, cho đến khi tin báo đó hoặc trạng thái mới được trình tại giao diện giữa bộ phận tiếp nhận tin báo cháy và hệ thống quản lý tin báo cháy.

3.1.3.5

Dấu thời gian (Time stamp)

Giá trị thời gian duy nhất được gán để xác định thời điểm cụ thể của một sự kiện.

3.1.4 Bảo mật và an toàn thông tin

3.1.4.1

Bảo mật tín hiệu (signalling security)

Các phương pháp được sử dụng để ngăn chặn hoặc phát hiện các hành vi cố ý can thiệp vào quá trình truyền tín hiệu.

CHÚ THÍCH: Các hành vi cố ý can thiệp vào quá trình truyền tín hiệu như chặn tín hiệu hoặc thay thế tín hiệu.

3.1.4.2

Mã hóa (encryption)

Là quá trình chuyển đổi luồng dữ liệu (luồng bit) sang định dạng mã hóa trước khi truyền, để thông tin chứa trong dữ liệu không thể bị giải mã bởi các bên không được phép.

3.1.4.3

Mức truy cập (access level)

Trạng thái của thiết bị, hệ thống, trong đó người dùng được truy cập thực hiện một hoặc một số hành động cụ thể, bao gồm:

- Vận hành các điều khiển;

- Thực hiện các thao tác thủ công;

- Quan sát các chỉ dẫn;

- Thu thập thông tin.

CHÚ THÍCH: Xem Phụ lục D để biết chi tiết phân loại mức truy cập.

3.1.4.4

Truy cập logic (logical access)

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

CHÚ THÍCH: Truy cập logic là khái niệm dùng để chỉ quyền truy cập vào hệ thống, thiết bị hoặc dữ liệu thông qua phần mềm, hệ điều hành hoặc mạng, thay vì tiếp cận vật lý trực tiếp đến thiết bị.

3.1.4.5

Vị trí an toàn (secure location)

Địa điểm đảm bảo yêu cầu về an ninh, an toàn theo quy định.

3.1.4.6

Xác thực (authentication)

Quá trình trao đổi mã nhằm xác minh rằng thiết bị truyền tin báo cháy chưa bị thay thế bằng thiết bị tương tự nhưng không có mã này hoặc thông tin truyền đi chưa bị sửa đổi.

3.2 Chữ viết tắt

Tiêu chuẩn này áp dụng các từ viết tắt sau đây

Ký hiệu	Diễn giải	
	Tiếng Việt	Tiếng Anh
FAMS	Hệ thống quản lý tin báo cháy	Fire alarm management system

FARC	Trung tâm tiếp nhận báo cháy	Fire alarm receiving centre
FATB	Khối truyền tin báo cháy	Fire alarm transmission block
FATP	Đường truyền tin báo cháy	Fire alarm transmission path
FATS	Hệ thống truyền tin báo cháy	Fire alarm transmission system
FATSN	Mạng dịch vụ truyền tin báo cháy	Fire alarm transmission service network
FATSP	Đơn vị cung cấp dịch vụ truyền tin báo cháy	Fire alarm transmission service provider
FDAS	Hệ thống báo cháy	Fire detection and alarm system
I_{RCT}	Giao diện giữa hệ thống quản lý tin báo cháy và bộ phận tiếp nhận tin báo cháy	Interface of the FAMS to the RCT
NTP	Giao thức thời gian mạng	Network Time Protocol
RCT	Bộ phận tiếp nhận tin báo cháy	Fire alarm receiving centre transceiver
SPT	Thiết bị truyền tin báo cháy	Supervised premises transceiver
UTC	Thời gian phối hợp quốc tế	Coordinated universal time

4 Quy định chung

4.1 Khi FATB có chức năng hoặc thiết bị được tích hợp vào FDAS hoặc FAMS thì các chức năng hoặc thiết bị tích hợp đó phải đáp ứng yêu cầu của tiêu chuẩn này.

4.2 Nếu thiết bị hoặc hệ thống có thêm các chức năng bổ sung ngoài phạm vi tiêu chuẩn này, các chức năng đó không được làm ảnh hưởng đến việc tuân thủ các yêu cầu quy định trong tiêu chuẩn này. Nhà sản xuất thiết bị hoặc hệ thống đó phải khai báo rõ các chức năng bổ sung và bảo đảm chúng phù hợp với các quy định của pháp luật hiện hành (nếu có).

4.3 Hệ thống và thiết bị quy định tại tiêu chuẩn này phải đáp ứng các yêu cầu về kết nối, thiết lập, chấm dứt kết nối và truyền tải theo quy định của pháp luật hiện hành.

5 Yêu cầu đối với mạng dịch vụ truyền tin báo cháy

5.1 Yêu cầu chung

5.1.1 Cấu hình của khối truyền tin báo cháy

5.1.1.1 FATB phải bảo đảm việc truyền các tin báo cháy và báo lỗi từ một hoặc nhiều FDAS tại một cơ sở được giám sát đến FARC thông qua các FATP theo quy định tại tiêu chuẩn này.

5.1.1.2 Cấu hình của FATB phải đáp ứng các quy định sau:

a) Có tối thiểu hai FATP, bao gồm một FATP chính và một FATP dự phòng, có thể vận hành luân phiên hoặc song song;

b) SPT phải có giao diện mạng chính và dự phòng, mỗi giao diện kết nối với một FATP độc lập;

c) Có RCT dự phòng;

d) Các RCT (kể cả RCT dự phòng) phải có giao diện mạng chính và giao diện mạng dự phòng, mỗi giao diện kết nối với một FATP độc lập;

e) Phải có FATSP chịu trách nhiệm giám sát, quản lý hiệu năng của FATB.

5.1.2 Đường truyền tin báo cháy

5.1.2.1 FATP có thể gồm nhiều loại liên kết truyền tin khác nhau, bao gồm:

a) Liên kết truyền tin có thể dùng chung với các ứng dụng không liên quan đến truyền tin báo cháy;

CHÚ THÍCH: Ứng dụng không liên quan đến truyền tin báo cháy là các ứng dụng không có chức năng truyền tin báo cháy nhưng sử dụng chung hạ tầng mạng (ví dụ các ứng dụng truyền dữ liệu văn phòng, dữ liệu camera giám sát, dịch vụ lưu trữ đám mây, cập nhật phần mềm tự động...).

b) Liên kết truyền tin truyền tải các đoạn của các FATP khác;

c) Thiết bị mạng truyền dẫn của bên thứ ba, thiết bị này không nằm ở cơ sở được giám sát hoặc FARC và không được phân loại là SPT hoặc RCT;

d) Thiết bị của bên thứ ba được đặt tại cơ sở được giám sát nhưng không được phân loại là SPT hoặc RCT.

5.1.2.2 Vì FATB có các FATP mang các liên kết truyền tin như trình bày tại 5.1.2.1 do đó hiệu năng của FATB có thể bị ảnh hưởng bởi các yếu tố: Dữ liệu đến không mong muốn, không đúng định dạng hoặc chủ ý phá hoại tại các giao diện của SPT hoặc RCT; tắc nghẽn mạng truyền dẫn do chia sẻ liên kết truyền tin hoặc mạng truyền dẫn không khả dụng do thiết bị hỏng và/hoặc bảo trì.

5.1.2.3 Liên kết truyền tin được chia sẻ với các ứng dụng khác

Các liên kết truyền tin được chia sẻ với các ứng dụng khác phải bảo đảm việc vận hành, bảo trì không ảnh hưởng đến các yêu cầu của FATB tại tiêu chuẩn này.

5.1.2.4 Thiết bị mạng truyền dẫn

Thiết bị mạng truyền dẫn trung gian giữa giao diện mạng của SPT và RCT không phải tuân theo các yêu cầu tại 5.2, 5.3 của tiêu chuẩn này.

CHÚ THÍCH 1: Ví dụ giao diện mạng tích hợp SPT bao gồm modem tương tự, 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.

CHÚ THÍCH 2: Các lỗi giao diện mạng cục bộ có thể được SPT phát hiện và gửi cảnh báo đến RCT bằng cách sử dụng FATP còn hoạt động. Tuy nhiên, việc giám sát giao diện mạng không thể được coi là xác nhận rằng FATP thực sự đang hoạt động.

5.1.2.5 Dung lượng của FATSN

FATSP phải công bố số lượng FDAS tối đa có thể kết nối với FATSN, sao cho bất kỳ FATP nào cũng vẫn đáp ứng các yêu cầu về thời gian truyền quy định tại 5.1.3.2, trong điều kiện hoạt động bình thường cũng như trong các điều kiện kiểm tra dưới đây:

a) Mỗi FDAS gửi một tin báo mỗi phút đến FATB. Số lượng FDAS phải tối thiểu là 0,1 % dung lượng FATSN, và

b) Tại giao diện giữa RCT và FAMS, FATB phải có khả năng tiếp nhận và chuyển tiếp tối thiểu 2 tin báo cháy mỗi phút.

5.1.2.6 Chống tấn công từ chối dịch vụ (DoS)

5.1.2.6.1 FATB phải tự bảo vệ khỏi các cuộc tấn công từ chối dịch vụ (DoS) từ mạng truyền dẫn.

5.1.2.6.2 Bất kỳ dạng dữ liệu hoặc tín hiệu nào nhận được từ mạng truyền dẫn cũng không được ảnh hưởng đến chức năng đã quy định của FATP, trừ khi lượng dữ liệu vượt quá khả năng xử lý của liên kết truyền tin dẫn đến tắc nghẽn mạng. Trong mọi trường hợp, không được giảm hiệu năng FATP nếu băng thông vẫn đủ để duy trì việc truyền tín hiệu.

5.1.2.6.3 Bất kỳ dữ liệu độc hại nào nhận được từ một giao diện mạng truyền dẫn đều không được gây ảnh hưởng đến hoạt động của SPT và RCT hoặc hoạt động của bất kỳ giao diện mạng truyền dẫn nào khác kể cả khi lượng dữ liệu độc hại chiếm toàn bộ băng thông, khiến giao diện đó không thể hoạt động.

5.1.2.6.4 Nếu hiệu năng của FATB bị ảnh hưởng bởi một cuộc tấn công DoS, tín hiệu lỗi phải được tạo ra theo các yêu cầu giám sát và báo cáo lỗi quy định tại Bảng 1.

CHÚ THÍCH 1: Yêu cầu này nhằm nhấn mạnh yêu 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 SPT và RCT. Các cuộc tấn công này có thể được thực hiện bằng cách sử dụng tín hiệu độc hại được thiết kế để làm suy yếu SPT, RCT hoặc bằng cách làm quá tải các thông tin liên lạc với lượng dữ liệu lớn.

CHÚ THÍCH 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: 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...

5.1.3 Hiệu năng của FATB

5.1.3.1 Hiệu năng của FATB phải được đánh giá dựa trên các tiêu chí về thời gian truyền, thời gian báo cáo lỗi, khả năng giám sát các kết nối và độ khả dụng.

5.1.3.2 Thời gian truyền

5.1.3.2.1 Thời gian truyền của FATB phải bảo đảm các yêu cầu sau:

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

b) Ít nhất 95 % các lần truyền phải có thời gian truyền không vượt quá 15 s;

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

5 1.3.2.2 Bất kỳ thời gian truyền nào vượt quá thời gian truyền lớn nhất sẽ được phân loại là một lỗi FATB với lưu ý tại 5.1.3.2.5.

5.1.3.2.3 Thời gian truyền được đo từ lúc thay đổi trạng thái hoặc tin báo (báo cháy, báo lỗi) được đưa ra để truyền tại giao diện giữa SPT và FDAS cho đến thời điểm tin báo đó hoặc trạng thái mới được trình bày tại giao diện giữa RCT và FAMS.

5.1.3.2.4 Thời gian truyền áp dụng cho tất cả các tin báo được truyền từ FDAS qua giao diện SPT tới

FATB.

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

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

CHÚ THÍCH 3: Thời gian xử lý trong FDAS được quy định trong các tiêu chuẩn khác.

CHÚ THÍCH 4: Thời gian truyền bao gồm cả thời gian thiết lập kết nối.

5.1.3.2.5 Khi thời gian truyền không thể đo trực tiếp thì có thể chấp nhận được bằng việc đo thời gian khứ hồi. Trong trường hợp này, thời gian truyền đo được bằng thời gian khứ hồi phải đáp ứng các yêu cầu tại 5.1.3.2.1 và Bảng 1.

CHÚ THÍCH 1: Thời gian truyền có thể khác đáng kể so với một nửa thời gian khứ hồi, do độ trễ và quá trình xử lý ở hai chiều không nhất thiết giống nhau.

CHÚ THÍCH 2: Thời gian khứ hồi là thời gian được đo từ khi xảy ra thay đổi trạng thái hoặc tin báo được trình bày để truyền tại giao diện của SPT với FDAS cho đến thời điểm tín hiệu hoặc thông báo xác nhận của RCT được trình bày tại giao diện của SPT với FDAS.

5.1.3.3 Giám sát các kết nối và báo cáo lỗi

5.1.3.3.1 Tất cả các kết nối sau đây của FATB phải được giám sát, phát hiện lỗi, báo cáo và ghi lại lỗi:

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

b) Giám sát đầu cuối FATP;

c) Giám sát kết nối RCT với FAMS.

5.1.3.3.2 Giám sát kết nối FDAS với SPT

Khi xảy ra lỗi kết nối giữa FDAS và SPT, tín hiệu lỗi phải được tạo ra và truyền đến FAMS có liên quan trong thời gian quy định tại 5.1.3.2.

5.1.3.3.3 Giám sát FATB

5.1.3.3.3.1 Mỗi FATP phải sử dụng một giao diện độc lập để kết nối SPT với các mạng truyền dẫn, nhằm đảm bảo một hành động phá hoại đơn lẻ không thể khiến tất cả các FATP bị gián đoạn cùng lúc. Một FATP sẽ được xác định là FATP chính, FATP còn lại sẽ được xác định là FATP dự phòng. Tất cả FATP sẽ được giám sát với thời gian báo cáo lỗi không được vượt quá các giá trị được quy định tại Bảng 1.

Bảng 1 - Thời gian báo cáo lỗi tối đa

STT	Các lỗi được giám sát	Thời gian báo cáo tối đa
1	FATP chính lỗi	90 s
2.	FATP chính hoạt động bình thường và xuất hiện lỗi tại FATP dự phòng	5 h
3.	FATP dự phòng đang lỗi và FATP chính xuất hiện lỗi	90s
4.	Tất cả các FATP lỗi cùng lúc	180 s

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

CHÚ THÍCH 2: Các lỗi giao diện mạng cục bộ có thể được SPT phát hiện và gửi cảnh báo đến RCT bằng cách sử dụng FATP còn hoạt động. Tuy nhiên, việc giám sát giao diện mạng không thể được coi là xác nhận rằng FATP thực sự đang hoạt động.

5.1.3.3.3.2 FATB phải báo cáo tất cả các lỗi FATB và lỗi FATP đến FAMS. Mọi lỗi FATB phải được báo cáo cho FATSP để kịp thời xử lý.

5.1.3.3.3.3 Các lỗi FATB phải được SPT phát hiện và chỉ báo.

CHÚ THÍCH: Không phải mọi lỗi FATP đều được xem là lỗi FATB. Hệ thống vẫn được coi là hoạt động bình thường nếu có ít nhất một FATP còn duy trì truyền tin trong thời gian quy định. Lỗi FATB được xác định khi toàn bộ các FATP trong hệ thống không còn đáp ứng yêu cầu tại tiêu chuẩn này.

5.1.3.3.4 Giám sát kết nối với FAMS

Kết nối giữa RCT và FAMS phải được giám sát. Nếu xảy ra lỗi kết nối, tín hiệu lỗi phải được tạo ra, ghi lại và gửi đến FAMS, RCT hoặc trung tâm giám sát có liên quan trong thời gian không quá 90 s.

5.1.4 Bảo đảm toàn vẹn mọi tin báo

Tin báo không được bị mất ngay cả trong trường hợp mất điện hoặc bất kỳ sự kiện nào khác do SPT hoặc RCT gây ra, ví dụ như khởi động lại phần mềm.

5.1.5 Xác nhận truyền tin báo

Phải có cơ chế để xác nhận rằng mỗi tin báo nhận được tại SPT từ FDAS hoặc do FATB tạo ra đều được chuyển đến FAMS một cách chính xác. Điều này có thể được thực hiện bằng cách RCT gửi một thông báo xác nhận về việc tin báo cháy hoặc báo lỗi đã được chuyển đến đích theo thời gian quy định, hoặc một thông báo lỗi sẽ được tạo ra khi tín hiệu không được chuyển đến đích hoặc thời gian xác nhận vượt quá quy định. Thông báo xác nhận hoặc thông báo lỗi phải được gửi đến SPT và được chỉ báo tại SPT.

5.1.6 Cảnh báo do FATB tạo ra

5.1.6.1 FATB phải báo cáo tất cả các lỗi FATB và FATP đến FAMS.

5.1.6.2 Khi FATB bị lỗi, một tin báo lỗi sẽ được tạo ra và được truyền đến FAMS có liên quan trong thời gian được quy định tại 5.1.3.2.

5.1.6.3 Khi FATB vẫn hoạt động, nếu có một FATP xảy ra lỗi, lỗi này phải được báo cho FATSP, có thể trì hoãn báo cho FAMS tối đa 96 h nếu FATSP và các bên liên quan thống nhất.

CHÚ THÍCH 1: FATSP phải lưu lại chính xác và đầy đủ nội dung các tin báo được sử dụng để báo cáo cho FAMS.

CHÚ THÍCH 2: Phương pháp báo cáo về tất cả các lỗi FATP đến FAMS phải là thông báo: “lỗi FATP chính của FATB”, “lỗi FATP dự phòng của FATB” và/hoặc “tất cả các FATP bị lỗi”. FATSP phải ghi lại phương pháp báo cáo.

5.1.7 Độ khả dụng

5.1.7.1 Độ khả dụng của FATP, FATB và FATSN là tỷ lệ phần trăm thời gian mà chúng hoạt động đảm bảo quy định tại tiêu chuẩn này. Trừ khi có tình huống báo cháy hoặc lỗi, FATB phải được giám sát để đảm bảo tính toàn vẹn. Việc giám sát phải được thực hiện với tần suất đủ để thời gian báo lỗi đáp ứng quy định tại Bảng 1. Phải cung cấp bằng chứng cho thấy độ khả dụng đã được ghi lại và có thể kiểm tra bất kỳ lúc nào.

CHÚ THÍCH 1: Không nên nhầm lẫn giữa độ khả dụng của FATP, FATB và FATSN với độ khả dụng của mạng truyền dẫn. Để tính toán độ khả dụng của FATP và FATB, cần xem xét độ khả dụng của ba thành phần chính: SPT, mạng truyền dẫn, và RCT theo dạng nối tiếp. Nghĩa là nếu bất kỳ thành phần nào trong ba thành phần này không hoạt động thì độ khả dụng tổng thể sẽ bị ảnh hưởng; chỉ khi cả ba cùng hoạt động bình thường thì FATP mới được xem là khả dụng.

CHÚ THÍCH 2: Trong tiêu chuẩn này, độ khả dụng của các FATP được coi là song song (xem Phụ lục C).

CHÚ THÍCH 3: Độ khả dụng của FATSN được sử dụng làm chỉ số để xác định hiệu năng của FATSN cho FATSP.

5.1.7.2 Tính dự phòng (sao chép)

Nếu SPT hoặc RCT có nhiều giao diện kết nối vào FATB thì FATB sẽ vẫn được coi là khả dụng ngay cả khi một hoặc nhiều giao diện này gặp sự cố, với hai điều kiện sau:

a) Phải bảo đảm luôn tồn tại ít nhất một FATP hoạt động bình thường giữa một giao diện của FDAS và một giao diện của FAMS, và

b) Phương thức sử dụng giao diện phải đáp ứng yêu cầu sau:

- Nếu sử dụng song song: Tất cả các giao diện đều được sử dụng đồng thời để gửi và nhận tin báo. Khi một giao diện lỗi, các giao diện còn lại vẫn tiếp tục hoạt động bình thường.

- Nếu sử dụng theo cấu hình giao diện chính - dự phòng: Tất cả các tin báo thường được truyền và nhận trên một giao diện chính ở mỗi đầu SPT và RCT. Khi giao diện chính xảy ra lỗi, hệ thống sẽ tự động chuyển sang giao diện dự phòng đã được cấu hình sẵn.

5.1.7.3 FATB không khả dụng

FATB sẽ được coi là không khả dụng khi xảy ra một trong các trường hợp sau:

a) Phát sinh bất kỳ lỗi nào của FATB khiến tin báo cháy hoặc báo lỗi không thể truyền đến FARC trong thời gian quy định tại tiêu chuẩn này;

b) FATB phải ngừng hoạt động mà không có phương án dự phòng thay thế.

5.1.7.4 Thời gian không khả dụng của FATB

Thời gian mà FATB được coi là không khả dụng là khoảng thời gian từ lần cuối cùng hệ thống được

xác nhận là hoạt động bình thường (tức là không có lỗi) cho đến thời điểm phát hiện lỗi, khắc phục lỗi và xác nhận hệ thống khả dụng trở lại.

CHÚ THÍCH: Những lỗi phát sinh do cố ý tấn công hoặc phá hoại hệ thống sẽ không tính vào thời gian không khả dụng, miễn là chúng được phát hiện và báo cáo trong thời gian quy định tại Bảng 1.

5.1.7.5 Ghi lại độ khả dụng của FATB

Để theo dõi và xác minh hiệu năng, phải ghi lại độ khả dụng của cả FATP và FATB. Khi độ khả dụng của FATB thấp hơn 99,8 % hoặc của FATP thấp hơn 95 % trong bất kỳ khoảng thời gian 7 ngày nào, phải ghi rõ trong hồ sơ độ khả dụng. FATSP phải thiết lập quy trình để cung cấp báo cáo độ khả dụng cho các bên liên quan nhằm mục đích duy trì mức hiệu năng theo yêu cầu (xem Phụ lục C).

5.1.7.6 Độ khả dụng của FATSN

Độ khả dụng hàng năm của FATSN không được thấp hơn 99,9 %. Nếu không đạt mức này, FATSN phải tự động ghi nhận lỗi không khả dụng.

5.1.8 Bảo mật

5.1.8.1 Yêu cầu chung

5.1.8.1.1 FATSP phải mô tả các biện pháp để bảo vệ FATB và các thành phần của nó (ví dụ: SPT, RCT) chống lại các cuộc tấn công ác ý và các tác động vô ý.

5.1.8.1.2 Để bảo đảm an toàn thông tin và chống giả mạo, các kỹ thuật mật mã phải được sử dụng. Khi sử dụng các thuật toán mã hóa đối xứng, độ dài khóa phải không nhỏ hơn 128 bit. Khi sử dụng các thuật toán khác, phải có mức độ an toàn mật mã tương đương. Bất kỳ hàm băm nào được sử dụng phải cho đầu ra tối thiểu 128 bit. Các khóa phải được thay đổi tự động, định kỳ và được hệ thống tạo ra ngẫu nhiên.

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

5.1.8.1.4 Các biện pháp bảo mật trên phải áp dụng cho tất cả dữ liệu và chức năng quản lý của FATB bao gồm cấu hình từ xa, thay đổi phần mềm hoặc chương trình cơ sở (firmware) của SPT và RCT.

5.1.8.2 Bảo mật chống giả mạo

5.1.8.2.1 FATB phải có cơ chế chống giả mạo nhằm ngăn chặn việc thay thế trái phép SPT bằng thiết bị khác có hình thức tương tự hoặc mô phỏng chức năng của SPT. Cơ chế này phải bảo đảm rằng chỉ các thiết bị SPT hợp lệ mới có thể kết nối vào FATB.

5.1.8.2.2 Mỗi SPT và RCT phải được gán một khóa xác thực duy nhất. Việc xác thực phải được thiết kế để đủ số lượng khóa riêng cần thiết, bảo đảm mỗi thiết bị được nhận diện duy nhất và không thể bị nhầm lẫn với các thiết bị khác.

5.1.8.3 Bảo mật thông tin

FATB phải có cơ chế bảo vệ thông tin để ngăn chặn việc đọc trái phép và phát hiện mọi hành vi sửa đổi trái phép thông tin được truyền đi.

5.1.9 Tài liệu hướng dẫn

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

5.2 Yêu cầu đối với thiết bị truyền tin báo cháy

5.2.1 Yêu cầu chức năng và vận hành

5.2.1.1 Xử lý tín hiệu

5.2.1.1.1 SPT phải có khả năng thực hiện các chức năng sau:

a) Nhận tín hiệu báo cháy và báo lỗi từ FDAS;

b) Nhận tín hiệu báo lỗi từ FATP;

c) Nhận tín hiệu xác nhận từ RCT;

d) Truyền tín hiệu báo cháy và báo lỗi từ FDAS tới RCT;

đ) Truyền tín hiệu báo lỗi đến RCT, bao gồm: lỗi FATP; lỗi kết nối giữa SPT với FDAS; lỗi nguồn điện chính và dự phòng của SPT.

5.2.1.1.2 Các chỉ báo và/hoặc dạng đầu ra của SPT không được rối loạn khi tiếp nhận đồng thời một hoặc nhiều tín hiệu như đã nêu tại 5.2.1.1.1.

5.2.1.1.3 SPT có thể được bố trí tách rời hoặc tích hợp với FDAS.

5.2.1.2 Trạng thái và chỉ báo trạng thái

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

a) Trạng thái báo cháy: Khi nhận được tín hiệu báo cháy từ FDAS;

b) Trạng thái báo lỗi: khi phát hiện một trong các lỗi sau: lỗi FDAS, lỗi kết nối giữa SPT và FDAS; lỗi FATP; lỗi trong SPT (ví dụ lỗi nguồn điện chính và dự phòng);

c) Trạng thái tĩnh lặng: khi SPT được cấp nguồn điện thích hợp và không có báo cháy hoặc báo lỗi nào như quy định tại mục a, b của 5.2.1.2.1 được chỉ báo.

5.2.1.2.2 Chỉ báo trạng thái của SPT

5.2.1.2.2.1 Trạng thái của SPT phải được chỉ báo bằng đèn báo chỉ thị riêng biệt và/ hoặc một trường trên màn hình hiển thị chữ số. Đèn chỉ báo phải lóe sáng khi SPT phát hiện trạng thái và hiển thị ổn định khi SPT nhận được xác nhận từ RCT rằng tín hiệu đó đã được tiếp nhận hợp lệ.

5.2.1.2.2.2 Nếu có thêm các chỉ báo phụ bổ trợ ngoài các chỉ báo bắt buộc, thì những chỉ báo phụ này không được gây hiểu nhầm hoặc dẫn đến diễn giải sai.

CHÚ THÍCH: Các chỉ báo bổ trợ có thể bao gồm đèn hoặc hiển thị báo hiệu tình trạng mạng, trạng thái cập nhật phần mềm, nhiệt độ thiết bị ...hoặc các thông tin khác. Những chỉ báo này nhằm mục đích cung cấp thông tin bổ sung và không thay thế cho các chỉ báo bắt buộc.

5.2.1.2.2.3 SPT phải ưu tiên xử lý và truyền các tín hiệu nhận được từ FDAS, trong đó tín hiệu báo cháy phải được xử lý với mức ưu tiên cao nhất. Khi có tín hiệu ưu tiên, các trạng thái khác phải được ẩn đi và có thể được hiển thị lại thông qua thao tác thủ công ở mức truy cập 1.

5.2.1.2.2.4 SPT phải tự động hủy bỏ trạng thái chỉ báo (ngừng hiển thị và báo cáo) sau khi tin báo đã được đặt lại tại FDAS hoặc lỗi đã được khắc phục. Việc đặt lại trạng thái tại SPT phải được thực hiện hoàn toàn tự động, không cần thao tác thủ công từ người dùng. Sau khi đặt lại, SPT phải chỉ báo chính xác các trạng thái tương ứng với bất kỳ tín hiệu nào nhận được.

5.2.1.3 Chế độ hoạt động của SPT

5.2.1.3.1 Khi nhận được tin báo từ FDAS, SPT phải bảo đảm an toàn cho các tin báo trước khi chuyển đến RCT. Tất cả các tin báo phải kèm dấu thời gian với độ phân giải quy định tại 5.2.1.12.4.

5.2.1.3.2 Để bảo đảm an toàn cho các tin báo nhận được từ FDAS trước khi chuyển đến RCT, SPT phải có bộ nhớ không mất dữ liệu (non-volatile), để lưu trữ các tin báo đó trong trường hợp mất điện hoặc FATB gặp sự cố. Các tin báo đã được SPT lưu trữ phải được truyền đến RCT ngay sau khi lỗi được khắc phục.

5.2.1.4 Giao diện với FDAS

5.2.1.4.1 Các kết nối với FDAS phải được SPT giám sát theo quy định tại 5.1.3.3.2. Thời gian tối đa để phát hiện và báo cáo lỗi giao diện không được vượt quá 90 s.

5.2.1.4.2 Có thể sử dụng bất kỳ loại giao diện nào giữa SPT và FDAS, miễn là đáp ứng yêu cầu của tiêu chuẩn này. Nhà sản xuất SPT phải công bố rõ trong tài liệu kỹ thuật loại giao diện sử dụng.

CHÚ THÍCH 1: Trong thực tế, các loại giao diện giữa SPT và FDAS có thể bao gồm:

- Giao diện song song: ví dụ như kết nối giữa tủ trung tâm báo cháy và thiết bị truyền tin báo cháy bằng tiếp điểm khô (NO/NC);

- Giao diện nối tiếp: ví dụ như kết nối qua cổng RS-232 hoặc RS-485 sử dụng giao thức chuẩn (như Modbus RTU, BACnet);

- Giao diện độc quyền: ví dụ như giao thức riêng của nhà sản xuất SPT, có thể thực hiện qua kết nối có dây (RS-485 với giao thức riêng) hoặc không dây (LoRa, Bluetooth,...), với điều kiện vẫn đáp ứng yêu cầu giám sát và an toàn quy định trong tiêu chuẩn;

CHÚ THÍCH 2: Để cho phép tương thích giữa các nhà sản xuất SPT khác nhau, Phụ lục G quy định hai loại giao diện nối tiếp và song song có thể có giữa FDAS và SPT.

5.2.1.5 Giám sát giao diện với mạng truyền dẫn

Nếu SPT có chức năng giám sát giao diện với mạng truyền dẫn và báo cáo lỗi cho RCT, tài liệu của nhà sản xuất SPT phải mô tả rõ cách thức thực hiện.

CHÚ THÍCH: Việc triển khai giám sát giao diện với mạng truyền dẫn không bắt buộc. Tuy nhiên, nó có thể hỗ trợ cho việc xác định và phân tích nguyên nhân gây ra lỗi FATP cho FATSP.

5.2.1.6 Cảnh báo do SPT tạo ra

SPT phải có khả năng tạo và truyền đến RCT các tin báo khi xảy ra lỗi cũng như khi lỗi đã được khắc phục sau:

a) Lỗi và khôi phục nguồn điện chính SPT;

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

c) Lỗi và khôi phục FATP chính;

d) Lỗi và khôi phục FATP dự phòng;

đ) Lỗi và khôi phục kết nối với FDAS.

5.2.1.7 Truy cập logic

5.2.1.7.1 Truy cập logic vào các chức năng của SPT phải đáp ứng các quy định sau:

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

b) Quyền truy cập mức 3 phải được ủy quyền bởi người dùng có quyền truy cập mức 2. Quyền truy cập mức 4 phải được ủy quyền bởi người dùng có quyền truy cập mức 3. Việc ủy quyền có thể thực hiện một lần như là một phần của thỏa thuận mức dịch vụ.

c) Phải bảo đảm khả năng cấp quyền truy cập mức 2, 3 và 4 với ít nhất một triệu tổ hợp khóa khác nhau.

5.2.1.7.2 Trong trường hợp có 3 lần truy cập không thành công trở lên trong vòng thời gian 60 s, SPT phải có khả năng trì hoãn các lần thử tiếp theo. Sau lần thứ ba, mỗi lần tiếp theo sẽ bị trì hoãn tối thiểu 90 s.

5.2.1.7.3 Trường hợp SPT được cung cấp khóa mặc định từ nhà sản xuất, việc cấu hình để đưa SPT vận hành sẽ không được hoàn tất nếu không thay đổi khóa mặc định này (ví dụ như trong quá trình cài đặt ban đầu). SPT phải được thiết kế sao cho không thể truy xuất, đọc lại hoặc trích xuất bất kỳ khóa truy cập nào được sử dụng để cấp quyền truy cập ở mức 2, mức 3 hoặc mức 4.

CHÚ THÍCH: Không thể truy xuất khóa nghĩa là khóa không được lưu trữ hoặc hiển thị dưới dạng có thể đọc được, dù từ giao diện thiết bị, phần mềm cấu hình hay tệp dữ liệu bên trong.

5.2.1.8 Bảo mật

Nhà sản xuất SPT phải cung cấp phương pháp bảo mật được sử dụng để chống giả mạo SPT và ngăn chặn việc đọc trái phép hoặc sửa đổi trái phép thông tin theo quy định tại 5.1.8.

5.2.1.9 Truy cập từ xa

Truy cập từ xa vào SPT phải đáp ứng tối thiểu các yêu cầu bảo mật thông tin quy định tại 5.1 của tiêu chuẩn này.

5.2.1.10 Tải lên, tải xuống phần mềm và chương trình cơ sở

5.2.1.10.1 Khi SPT có chức năng tải lên và tải xuống phần mềm hoặc chương trình cơ sở, chỉ những người dùng có mức truy cập phù hợp như quy định tại Phụ lục D và 5.2.1.7 mới được phép thực hiện chức năng này.

5.2.1.10.2 Phiên bản phần mềm dự kiến bị thay thế phải được lưu trước khi thực hiện tải xuống phiên bản mới. Nếu quá trình tải xuống bị gián đoạn do mất kết nối hoặc lỗi truyền dữ liệu, phiên bản phần mềm cuối cùng đã hoạt động ổn định phải được khôi phục và SPT phải trở lại trạng thái hoạt động như trước khi quá trình tải xuống bị gián đoạn.

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

5.2.1.11 Lưu trữ các tham số

Quá trình cấp nguồn lại (ví dụ: sau khi mất điện và được khôi phục) hoặc khởi động lại SPT không được làm mất bất kỳ dữ liệu cấu hình đặc thù nào của cơ sở. SPT phải trở lại trạng thái hoạt động bình thường sau các quá trình này.

CHÚ THÍCH: Dữ liệu cấu hình đặc thù của cơ sở (site specific data) là những dữ liệu phục vụ cho mục đích định danh, kiểm soát truy cập, xử lý và truyền tải chính xác các tin báo từ cơ sở được giám sát. Những dữ liệu này có thể gồm: Mã định danh của SPT; tên, địa chỉ cơ sở được giám sát; độ ưu tiên xử lý các tin báo; thông tin bảo mật và xác thực...

5.2.1.12 Ghi nhật ký sự kiện

5.2.1.12.1 SPT phải có khả năng lưu trữ các sự kiện được quy định tại Bảng 2.

CHÚ THÍCH: SPT không bắt buộc phải có toàn bộ chức năng liên quan đến các sự kiện trong Bảng 2, nhưng phải ghi lại được nếu có phát sinh.

5.2.1.12.2 Bộ nhớ phải có khả năng lưu trữ tối thiểu 1 000 sự kiện và phải được bảo vệ chống lại việc xóa hoặc thay đổi nội dung dù vô ý hay cố ý. Bộ nhớ phải có thời gian lưu trữ sự kiện tối thiểu 30 ngày sau khi SPT mất điện.

5.2.1.12.3 Nếu SPT tích hợp cùng FDAS, có thể sử dụng chung bộ nhớ nhật ký miễn là dung lượng và thời gian lưu trữ đáp ứng các yêu cầu tại 5.2.1.12.2.

5.2.1.12.4 Mỗi sự kiện lưu trữ phải được gắn dấu thời gian với độ phân giải tối thiểu là 1 s. Thời gian ghi nhận phải chính xác so với giờ UTC với sai số không quá ± 5 s. SPT phải cung cấp phương pháp hiệu chỉnh ngày và giờ để đồng bộ hóa thiết bị với thời gian chính xác.

CHÚ THÍCH: Độ phân giải tối thiểu là 1 s nghĩa là nếu hai sự kiện cách nhau 1 s hoặc hơn, thì phải được ghi nhận là hai thời điểm khác nhau.

5.2.1.12.5 SPT phải ghi lại tất cả các sự kiện khác nhau. Với các sự kiện lặp đi lặp lại giống nhau trong vòng 12 h chỉ cần ghi lại sự kiện đầu tiên và cuối cùng kèm theo số lần lặp lại.

5.2.1.12.6 Truy cập vào các thông tin nhật ký sự kiện phải yêu cầu xác thực người dùng.

Bảng 2 - Sự kiện cần ghi của SPT

STT	Sự kiện cần ghi
1.	Tin báo (báo cháy, báo lỗi) từ FDAS
2.	Thông báo từ RCT về việc đã nhận thành công tin báo từ SPT
3.	Thời gian chờ thông báo xác nhận từ RCT vượt quá quy định, hoặc thông báo từ RCT từ chối tiếp nhận tin báo từ SPT do lỗi hoặc không đúng định dạng
4.	Lỗi và khôi phục nguồn điện chính của SPT
5.	Lỗi và khôi phục nguồn điện dự phòng của SPT
6.	Lỗi và khôi phục kết nối giữa FDAS và SPT
7.	Lỗi và khôi phục FATP
8.	Lỗi và khôi phục FATB
9.	Lỗi và khôi phục giao diện SPT với mạng truyền dẫn
10.	Thay đổi cấu hình của SPT
11.	Bật nguồn hoặc thiết lập lại SPT
12.	Thay đổi phần mềm SPT
13.	Thay đổi thủ công ngày và giờ
14.	Truy cập vào SPT ở mức truy cập 2, 3 hoặc 4

5.2.2 Yêu cầu thiết kế

5.2.2.1 Công bố của nhà sản xuất

SPT phải đáp ứng quy định tại 5.2.2 đối với công nghệ được áp dụng. Để hỗ trợ cho quá trình đánh giá thiết kế, nhà sản xuất SPT phải công bố bằng văn bản rằng:

a) Việc thiết kế được thực hiện trong khuôn khổ một hệ thống quản lý chất lượng có tích hợp các nguyên tắc thiết kế tổng thể, ví dụ như ISO 9001;

b) Các linh kiện của SPT được lựa chọn phù hợp với mục đích sử dụng đã định và dự kiến vận hành trong giới hạn kỹ thuật tại môi trường bên ngoài vỏ bọc, đáp ứng yêu cầu cấp môi trường 3k5 theo TCVN 7921-3-3.

5.2.2.2 Hồ sơ thiết kế và tài liệu kỹ thuật

5.2.2.2.1 Nhà sản xuất SPT phải chuẩn bị hồ sơ về lắp đặt và hướng dẫn sử dụng, cung cấp kèm theo SPT cho đơn vị thử nghiệm. Hồ sơ phải bao gồm ít nhất các nội dung sau:

a) Một bản mô tả chung về thiết bị, bao gồm:

- Các chức năng tùy chọn theo tiêu chuẩn này;

- Các chức năng liên quan đến tiêu chuẩn, quy chuẩn hoặc quy định hiện hành khác về hệ thống báo cháy;

- Các chức năng bổ sung không quy định tại tiêu chuẩn này.

b) Các mô tả thông số kỹ thuật của đầu vào và đầu ra của SPT nhằm đánh giá về tính cơ học, điện và tính tương thích của phần mềm với FDAS, bao gồm:

- Các yêu cầu về nguồn điện (chính và dự phòng) đảm bảo cho SPT hoạt động theo khuyến cáo;

- Số lượng tối đa FDAS có thể kết nối, các vùng và/hoặc các điểm kết nối;

- Các loại giao diện FDAS mà SPT phù hợp;

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

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

- Cách thức giám sát giao diện mạng truyền dẫn;

- 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;

- 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 FATP;

- Các thông số khuyến cáo về dây dẫn cho mỗi FATP;

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

c) Các thông tin về lắp đặt, bao gồm:

- Tính phù hợp khi sử dụng ở các điều kiện môi trường khác nhau;

- Phương pháp bảo đảm tuân thủ 5.2.2.3;

- Hướng dẫn lắp đặt, đấu nối đầu vào và đầu ra.

d) Hướng dẫn cấu hình, chạy thử, vận hành, khai thác và bảo trì.

đ) Phương pháp xác định hiệu năng của FATB theo quy định tại tiêu chuẩn này.

5.2.2.2.2 Nhà sản xuất SPT phải cung cấp cho đơn vị thử nghiệm hồ sơ thiết kế chi tiết, 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 đối với thiết kế phần điện và phần cơ.

5.2.2.3 Thiết kế phần cơ

5.2.2.3.1 Vỏ bọc của SPT phải có kết cấu chắc chắn, phù hợp với phương pháp lắp đặt mô tả trong hồ sơ thiết kế. Vỏ bọc phải đạt tối thiểu cấp bảo vệ IP 30 theo TCVN 4255 (IEC 60529).

5.2.2.3.2 SPT có thể được đặt trong hai vỏ bọc trở lên ở các vị trí khác nhau, với yêu cầu mọi nút ấn thủ công và đèn chỉ báo bắt buộc phải đặt trên cùng một vỏ hoặc các vỏ liền kề.

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

5.2.2.3.4 Các vị trí đấu nối và cầu chì phải được dán nhãn rõ ràng.

5.2.2.4 Thiết kế phần điện và thiết kế khác

5.2.2.4.1 SPT phải được cấp nguồn từ 2 nguồn điện độc lập. Trong đó nguồn chính lấy điện từ lưới điện, nguồn điện dự phòng có thể từ nguồn điện của hệ thống báo cháy hoặc bằng nguồn riêng tích hợp. Cả hai nguồn phải đáp ứng TCVN 7568-4 (ISO 7240-4), trong đó nguồn dự phòng phải bảo đảm đủ cho SPT hoạt động bình thường ít nhất 24 h ở chế độ tĩnh và 30 min ở các trạng thái còn lại.

5.2.2.4.2 Có thể sử dụng một FATP để phát tín hiệu về một lỗi trên FATP khác.

5.2.2.4.3 Nếu SPT đặt phân tán trong nhiều vỏ bọc, cần có biện pháp đảm bảo rằng lỗi ngắn mạch hoặc đứt kết nối giữa các vỏ bọc không làm ảnh hưởng quá một chức năng trong thời gian vượt quá 90 s tính từ khi xảy ra lỗi.

5.2.2.4.4 Nếu SPT được thiết kế sử dụng nguồn cấp từ ngoài vỏ bọc chính, phải có ít nhất 2 đường cấp nguồn riêng biệt, sao cho nếu một trong các đường cấp nguồn đó bị ngắn mạch hoặc hở mạch thì việc cấp nguồn đến SPT vẫn được đảm bảo.

5.2.2.4.5 Việc chuyển đổi giữa nguồn cấp điện chính và nguồn điện dự phòng không được làm thay đổi bất kỳ chỉ báo hoặc tình trạng đầu ra nào, trừ các chỉ báo cấp nguồn.

5.2.2.4.6 Nếu SPT có cơ chế ngắt kết nối hoặc hiệu chỉnh nguồn điện chính và dự phòng, thì chỉ có thể thực hiện được ở mức truy cập 3 hoặc 4.

5.2.2.5 Khả năng tiếp cận đến các chỉ báo và bộ điều khiển

5.2.2.5.1 Sự phân cấp chức năng theo các mức truy cập phải đảm bảo ngăn chặn truy cập trái phép vào các mức truy cập cao hơn, nhưng cho phép truy cập hợp lệ vào mức truy cập thấp hơn. Các nút ấn thủ công và các chức năng khác phải được nhóm lại theo mức truy cập phù hợp quy định tại tiêu chuẩn này, cụ thể:

5.2.2.5.2 Tất cả các chỉ báo bắt buộc phải quan sát được ở mức truy cập 1 mà không cần bất kỳ thao tác thủ công (ví dụ như phải mở thiết bị).

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

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

5.2.2.5.5 Truy cập vào mức truy cập 2 phải được giới hạn bởi một quy trình bảo vệ đặc biệt.

5.2.2.5.6 Truy cập vào mức truy cập 3 phải được giới hạn bởi một quy trình bảo vệ đặc biệt, khác với quy trình đã áp dụng cho mức truy cập 2.

5.2.2.5.7 Truy cập vào mức truy cập 4 chỉ được thực hiện thông qua phương tiện đặc biệt không tích hợp trong thành phần của SPT.

CHÚ THÍCH: Phương tiện đặc biệt ở đây là các công cụ hoặc thiết bị chuyên dụng do nhà sản xuất SPT cung cấp, dùng để truy cập mức 4. Các công cụ này không được tích hợp sẵn trong SPT và chỉ do kỹ thuật viên hoặc cá nhân được ủy quyền sử dụng, ví dụ: máy tính cài phần mềm cấu hình đặc biệt, thiết bị lập trình, khóa bảo mật USB/smartcard hoặc các cơ chế xác thực phần cứng tương tự. Quy định này nhằm ngăn chặn truy cập trái phép vào mức quyền cao nhất, bảo đảm an toàn và tính toàn vẹn hoạt động của SPT.

5.2.2.6 Các chỉ báo

5.2.2.6.1 Chỉ báo bằng các đèn tín hiệu nhấp nháy

5.2.2.6.1.1 Chỉ báo bắt buộc từ các đèn tín hiệu nhấp nháy phải có khả năng nhìn thấy được trong điều kiện môi trường bình thường có cường độ ánh sáng đến 500 lx từ mọi góc nhìn lên đến 22,5° theo phương vuông góc với bề mặt lắp đặt, tại các khoảng cách như sau:

a) 3 m đối với các chỉ báo chung về trạng thái chức năng và chỉ báo về cung cấp nguồn điện;

b) 0,8 m đối với các chỉ báo khác.

5.2.2.6.1.2 Đối với các chỉ báo lóe sáng, thì cả chu kỳ bật và chu kỳ tắt 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 chỉ báo cháy;

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

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

a) Màu đỏ dùng cho chỉ báo cháy;

b) Màu vàng dùng cho chỉ báo trạng thái còn lại;

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

5.2.2.6.2 Chỉ báo trên màn hình chữ-số

5.2.2.6.2.1 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.

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

5.2.2.6.2.3 Nếu mục đích của mỗi trường hiển thị không thể hiện trực tiếp trên nội dung thì trường hiển thị đó phải có nhãn chỉ dẫn rõ ràng.

5.2.2.6.2.4 Sau khi có sự kiện báo cháy hoặc báo lỗi mới, thông tin bắt buộc phải được hiển thị rõ ràng liên tục trong vòng một giờ hoặc suốt thời gian cấp nguồn dự phòng, ở khoảng cách 0,8 m trong điều kiện ánh sáng có cường độ từ 5 lx đến 500 lx và theo bất kỳ góc nhìn nào tính từ tia vuông góc với mặt phẳng của màn hình quy định tại a), b) mục này. Sau 1 h hoặc hết thời gian nguồn 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 tại a), b) mục này. Nếu cần, phải cho phép người dùng điều chỉnh độ rõ bằng thao tác ở mức truy cập 1.

a) đến 22,5° khi nhìn từ mỗi cạnh bên, hoặc

b) đến 15° khi nhìn từ phía trên và phía dưới.

5.2.2.6.3 Đối với chỉ báo trên màn hình chữ-số không yêu cầu phải sử dụng các màu sắc khác nhau. Tuy nhiên nếu sử dụng thì phải tuân theo quy định về màu sắc tại 5.2.2.6.1.3.

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

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

SPT có thể tích hợp các bộ phận được điều khiển bằng phần mềm để đáp ứng các yêu cầu nêu tại tiêu chuẩn này. Trong trường hợp đó, SPT phải tuân thủ mục 5.2.3 liên quan đến công nghệ được sử dụng.

CHÚ THÍCH: Các bộ phận điều khiển bằng phần mềm có thể được cung cấp bởi bên thứ ba 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 ba được thiết kế và sản xuất cho SPT phải được lưu hồ sơ đầy đủ, Bên thứ ba sản xuất các bộ phận điều khiển bằng phần mềm 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 chức năng chính phải rõ ràng, được mô tả một cách tổng hợp và hồ sơ này phải luôn sẵn sàng để cung cấp cho đơn vị thử nghiệm.

5.2.3.2 Hồ sơ về phần mềm

5.2.3.2.1 Nhà sản xuất SPT 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 cùng với SPT. Hồ sơ này phải đảm bảo chi tiết đến mức thiết kế có thể được kiểm tra về sự phù hợp với tiêu chuẩn này.

5.2.3.2.2 Nhà sản xuất SPT phải chuẩn bị và duy trì hồ sơ thiết kế chi tiết. Hồ sơ này không bắt buộc phải cung cấp cho đơn vị thử nghiệm, nhưng phải được lưu giữ để sẵn sàng phục vụ kiểm tra khi cần thiết, đồng thời bảo đảm quyền bảo mật thông tin của nhà sản xuất.

5.2.3.3 Thiết kế phần mềm

Phần mềm trong SPT phải được thiết kế đảm bảo không xảy ra tình trạng khóa chết trong luồng chương trình, nhằm duy trì độ tin cậy vận hành.

5.2.3.4 Giám sát chương trình

5.2.3.4.1 Quá trình chạy của một chương trình phải được giám sát. Thiết bị giám sát phải 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 thực thi trong khoảng thời gian tối đa 100 s. Thiết bị giám sát phải có bộ đếm thời gian riêng độc lập với bộ đếm của hệ thống đang được giám sát.

5.2.3.4.2 Việc xảy ra lỗi trong hệ thống giám sát không được ảnh hưởng đến hoạt động giám sát hoặc khả năng phát hiện và báo lỗi hệ thống.

CHÚ THÍCH: Phần mềm giám sát bao gồm cả các chương trình trên nhiều bộ xử lý hoặc các phần mềm từ bên thứ ba. Trong trường hợp có mô-đun hiển thị 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 xem là đủ để kiểm tra.

5.2.3.5 Lưu các chương trình và dữ liệu

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

5.2.3.5.2 Chương trình phải được lưu giữ trong một bộ nhớ không mất dữ liệu 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.

5.2.3.5.3 Đối với các dữ liệu cấu hình đặc thù của cơ sở, phải đáp ứng các yêu cầu sau:

a) Việc thay đổi dữ liệu chỉ cho phép thực hiện ở mức truy cập 3 hoặc 4;

b) Việc thay đổi dữ liệu không được ảnh hưởng đến cấu trúc của phần mềm;

c) Nếu dữ liệu được lưu giữ trong bộ nhớ không mất dữ liệu, phải có nguồn dự phòng đảm bảo duy trì dữ liệu trong ít nhất hai tuần. Việc ngắt nguồn dự phòng chỉ được phép thực hiện ở mức truy cập 4;

d) Nếu dữ liệu được lưu giữ trong bộ nhớ đọc-ghi, phải có cơ chế để ngăn chặn việc ghi vào bộ nhớ trong quá trình vận hành ở mức truy cập 1 nhằm đảm bảo nội dung của bộ nhớ được bảo vệ khi xảy ra một lỗi trong quá trình chạy chương trình;

đ) Dữ liệu phải được cung cấp một tham chiếu về phiên bản và phải được cập nhật mỗi khi thực hiện thay đổi một bộ thông số;

e) Tham chiếu về phiên bản của dữ liệu chỉ có thể truy xuất ở mức truy cập 3.

5.2.3.6 Giám sát nội dung bộ nhớ

Toàn bộ nội dung bộ nhớ chứa dữ liệu cấu hình đặc thù của cơ sở được giám sát phải được kiểm tra định kỳ không quá một giờ. Hệ thống phải báo lỗi nếu phát hiện bất kỳ sự mâu thuẫn nào trong dữ liệu lưu trữ.

5.2.4 Yêu cầu về ghi nhãn

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

a) Tên hoặc nhãn hiệu của nhà sản xuất;

b) Số hiệu về loại hoặc ký hiệu khác của SPT.

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

5.3 Yêu cầu đối với bộ phận tiếp nhận tin báo cháy

5.3.1 Yêu cầu chung

5.3.1.1 RCT có chức năng giám sát FATB, nhận và chuyển tiếp tin báo cháy và báo lỗi đến FAMS, đồng thời gửi tín hiệu xác nhận đến SPT. RCT phải giám sát giao diện với FAMS và đảm bảo khả năng liên lạc giữa FAMS với một hoặc nhiều SPT.

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

5.3.2 Yêu cầu về quyền truy cập logic.

5.3.2.1 Truy cập vào mọi chức năng của RCT đều phải thông qua ủy quyền bằng khóa.

5.3.2.2 Mức truy cập 2, 3 và 4 sẽ phải thực hiện bằng tài khoản cá nhân để đảm bảo khả năng truy xuất các hành động đã thực hiện. Người dùng có quyền truy cập mức độ 4 sẽ được người dùng có quyền truy cập mức độ 3 ủy quyền, quyền này có thể vĩnh viễn hoặc theo thời hạn.

5.3.2.3 Truy cập ở mọi mức độ phải được ủy quyền bằng khóa. Cơ chế tạo khóa phải có khả năng tạo ra ít nhất 1 000 000 khóa khác nhau.

5.3.2.4 Trong trường hợp nếu có 3 lần truy cập không thành công trở lên trong vòng thời gian 60 s, RCT phải có khả năng trì hoãn các lần thử tiếp theo. Sau lần thứ ba, mỗi lần tiếp theo sẽ bị trì hoãn tối thiểu 90 s. Sự kiện này phải được ghi nhận và gửi cảnh báo tới FATSP, hành vi này phải bị coi là hành vi cố ý tấn công hệ thống.

5.3.2.5 Nếu RCT có khóa mặc định từ nhà sản xuất, việc cấu hình để đưa RCT vận hành sẽ không thể hoàn tất nếu không thay đổi khóa mặc định này (ví dụ: trong quá trình cài đặt).

5.3.2.6 Truy cập từ xa chỉ được phép khi sử dụng kết nối an toàn và đáp ứng các yêu cầu bảo mật theo quy định tại 5.1.

5.3.2.7 Hệ thống phải tự động đăng xuất khỏi các phiên truy cập từ xa sau một thời gian không hoạt động. Khoảng thời gian này có thể cấu hình được để phù hợp yêu cầu bảo mật.

5.3.2.8 Phân quyền từng mức truy cập vào các chức năng được nêu tại Bảng 3

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

Mức truy cập	Mức 1	Mức 2	Mức 3	Mức 4
Xem các chỉ báo 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, tin báo cháy, báo lỗi của 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
CHÚ THÍCH: Yêu cầu “không” hoặc “cho phép” truy cập vào một chức năng nhất định không có nghĩa là chức năng đó bắt buộc phải tồn tại.				

5.3.3 Tải lên và tải xuống phần mềm

Việc tải lên và tải xuống phần mềm đối với RCT chỉ được phép ở mức truy cập phù hợp như quy định tại 5.3.2 và Phụ lục D.

5.3.4 Lưu trữ các tham số và dữ liệu

Quá trình cấp nguồn lại (ví dụ sau khi mất điện và được khôi phục) 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 tin báo đã được bảo vệ nào. RCT phải tự động trở lại trạng thái hoạt động bình thường sau các quá trình này.

5.3.5 Giám sát và thông báo lỗi của FATP và FATB

RCT phải giám sát FATP và FATB. Khi phát hiện lỗi, RCT phải gửi tin báo lỗi đến FAMS và FATSP theo quy định tại 5.1. Nhà sản xuất RCT phải cung cấp tài liệu mô tả chi tiết tín hiệu lỗi.

5.3.6 Giao diện với FAMS

5.3.6.1 Các giao diện với FAMS phải được giám sát theo 5.1. Thời gian báo cáo lỗi kết nối phải nhỏ hơn hoặc bằng thời gian báo cáo lỗi của FATB, hoặc 60 s, tùy theo giá trị thời gian nào nhỏ hơn. Trong trường hợp lỗi giao diện, tín hiệu lỗi sẽ được tạo ra và sự kiện sẽ được ghi lại.

5.3.6.2 Nhà sản xuất RCT phải mô tả trong tài liệu sản phẩm các thông số kỹ thuật của giao diện đầu ra của RCT để kết nối với FAMS, cũng như cách thức tín hiệu lỗi được hiển thị và ghi nhận

5.3.6.3 Có thể cung cấp giao diện dự phòng tại đầu ra tại RCT để kết nối với FAMS.

5.3.7 Tín hiệu lỗi

5.3.7.1 RCT phải có cơ chế báo lỗi trong các trường hợp sau:

a) Lỗi mất liên kết truyền tin giữa RCT và FAMS thông qua giao diện I_{RCT};

CHÚ THÍCH: Lỗi này có thể không cần gửi tới FAMS nếu FATP đã bị lỗi.

b) Lỗi giao diện mạng truyền dẫn giữa RCT và SPT (ví dụ lỗi mã hóa);

c) Lỗi nội bộ bên trong RCT, bao gồm cả sai lệch thời gian sau khi đưa vào vận hành.

5.3.7.2 Nhà sản xuất RCT phải mô tả trong tài liệu cơ chế báo lỗi cho FAMS, FATSP và cách thức kiểm tra cơ chế báo lỗi này.

5.3.8 Ghi nhật ký sự kiện

5.3.8.1 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.

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

5.3.8.3 Bộ nhớ lưu nhật ký phải là loại không mất dữ liệu, với thời gian lưu giữ tối thiểu 3 năm. Nhà sản xuất RCT phải nêu rõ trong tài liệu của họ cách thức thực hiện điều này.

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

5.3.8.5 Ngoài sự kiện, nhật ký phải kèm dấu thời gian sự kiện xảy ra với độ phân giải thời gian tối thiểu 1 s và sai số so với UTC không quá ± 5 s.

5.3.8.6 RCT phải có khả năng đồng bộ thời gian với UTC và có thể sử dụng múi giờ địa phương. Nhà sản xuất RCT phải chỉ rõ trong tài liệu của họ cách đồng bộ hóa thời gian với UTC.

5.3.8.7 Để tối ưu hóa việc lưu trữ sự kiện, nếu các sự kiện giống hệt nhau xảy ra trong khoảng thời gian liên tục 12h nào thì chỉ cần ghi sự kiện đầu và sự kiện cuối, cùng số lượng các sự kiện giống nhau.

5.3.8.8 Các sự kiện có yêu cầu bắt buộc nhận dạng người dùng tại Bảng 4, việc ghi nhật ký truy cập vào RCT phải bao gồm nhận dạng người dùng.

Bảng 4 - Sự kiện cần ghi của RCT

STT	Sự kiện cần ghi	Nhận dạng người dùng
1	Tin báo cháy và báo lỗi từ FATB	Không bắt buộc
2	Lỗi và khôi phục kết nối với FAMS	Không bắt buộc
3	Lỗi và khôi phục giao diện mạng truyền dẫn	Không bắt buộc
4	Thay đổi cấu hình RCT	Bắt buộc
5	Bật nguồn hoặc khởi động lại	Bắt buộc
6	Bất kỳ thay đổi nào đối với phần mềm của RCT	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 truy cập của người dùng	Bắt buộc
CHÚ THÍCH: Việc ghi lại thông tin nhận dạng người dùng chỉ bắt buộc nếu sự kiện phát sinh do hành động can thiệp của người dùng.		

5.3.9 Chế độ vận hành của RCT

5.3.9.1 RCT có thể vận hành ở hai chế độ: Lưu và chuyển tiếp; hoặc truyền thẳng. Nhà sản xuất RCT phải mô tả rõ trong tài liệu RCT những chế độ vận hành nào được hỗ trợ.

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

5.3.9.2.1 Khi nhận được tin báo từ SPT, RCT phải lưu trữ an toàn các tin báo này và gửi xác nhận đã nhận được tin báo cho SPT.

5.3.9.2.2 Tất cả các tin báo phải bao gồm dấu thời gian tại thời điểm SPT nhận được hoặc tạo ra.

5.3.9.2.3 RCT cũng phải ghi lại dấu thời gian khi tin báo được chuyển tiếp từ RCT đến FAMS và/hoặc

khi nhận được xác nhận từ FAMS.

5.3.9.2.4 Tin báo phải được lưu trữ trong bộ nhớ không mất dữ liệu của RCT nhằm bảo vệ các tin báo đã được xác nhận nếu giao diện với FAMS bị lỗi hoặc khi mất điện. Các tin báo đã lưu trữ sẽ được truyền đi khi tình trạng lỗi được khắc phục.

5.3.9.2.5 Tin báo đã được lưu trữ sẽ được truyền đến FAMS. FAMS sẽ không gửi xác nhận cho SPT, vì do RCT đã thực hiện việc này.

CHÚ THÍCH: Việc mất tin báo được coi là tình huống xấu hơn so với việc gửi tin bị chậm trễ.

5.3.9.3 Yêu cầu đối với chế độ vận hành truyền thẳng

5.3.9.3.1 Khi nhận được tin báo (báo cháy, báo lỗi) từ SPT, RCT sẽ phải chuyển tiếp đến FAMS.

5.3.9.3.2 RCT chỉ gửi xác nhận cho SPT, sau khi đã được FAMS xác nhận đã nhận được tin báo.

5.3.10 Chống tấn công từ chối dịch vụ

Nhà sản xuất RCT phải cung cấp phương pháp được sử dụng để đảm bảo đáp ứng quy định tại 5.1.2.6.

5.3.11 Bảo mật thông tin

Nhà sản xuất RCT phải cung cấp phương pháp được sử dụng để đảm bảo đáp ứng quy định tại 5.1.8, áp dụng cho cả giao tiếp của SPT và truy cập từ xa.

5.3.12 Bảo mật chống giả mạo

Nhà sản xuất RCT phải cung cấp phương pháp được sử dụng đề đảm bảo đáp ứng quy định tại 5.1.8

5.3.13 RCT dự phòng

Nhà sản xuất RCT phải chỉ rõ và chứng minh việc đảm bảo dự phòng RCT theo quy định tại 5.1.1.

5.3.14 Tài liệu

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

5.3.14.2 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.

5.3.14.3 Trong trường hợp có các bộ phận mà người dùng có thể tự bảo dưỡng (ví dụ cầu chì), loại và thông số kỹ thuật của chúng sẽ được cung cấp.

5.3.14.4 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) Loại FAMS phù hợp;

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

g) Số lượng tin báo tối đa có thể xử lý được mỗi giây;

h) Danh sách các danh mục FATB được hỗ trợ;

i) Yêu cầu về nguồn điện.

5.3.15 Ghi nhãn

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

- Tên hoặc dấu hiệu của nhà sản xuất;

- Mã nhận dạng sản phẩm (nếu có);

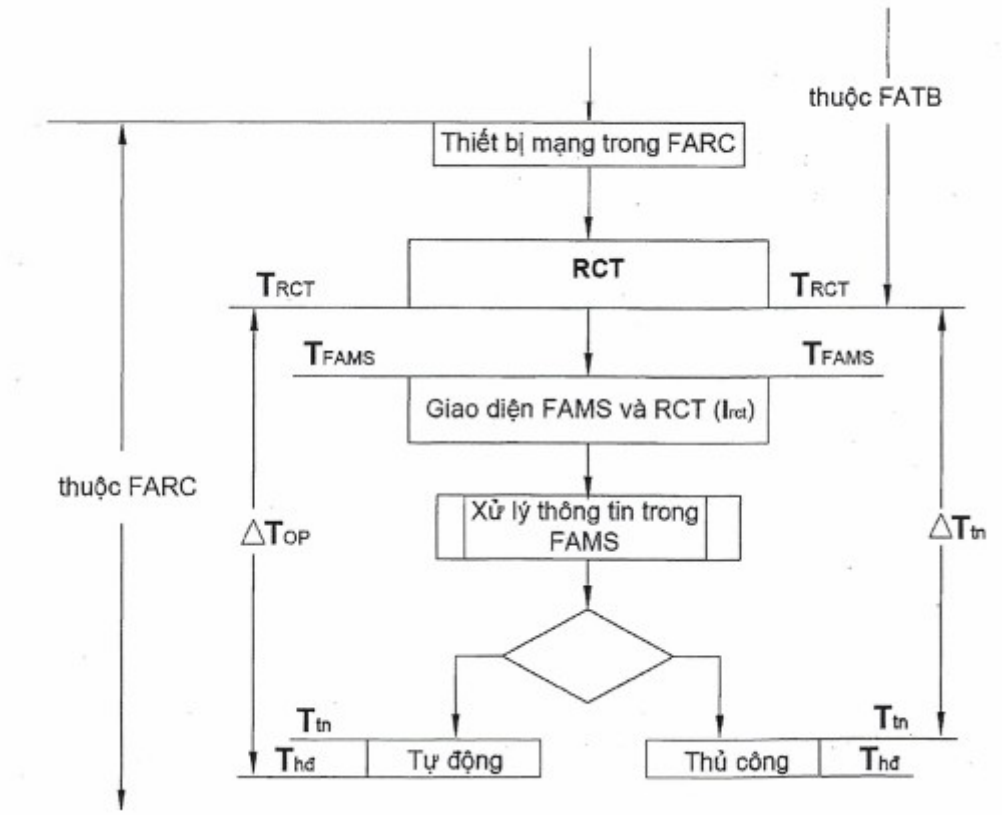
- Sự phù hợp với tiêu chuẩn này

5.3.15.2 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 5.3.15.1.

6 Yêu cầu đối với trung tâm tiếp nhận báo cháy

6.1 Xử lý tin báo

6.1.1 Quá trình xử lý các tin báo tại FARC được mô tả như hình 1.



Hình 1 - Quá trình xử lý thông tin tại FARC

CHÚ DẪN:

- T_{RCT}: Thời điểm RCT bắt đầu gửi tin báo đến FAMS.

- T_{FAMS}: Thời điểm FAMS nhận tin báo.

- T_{tn}: Thời điểm nhân viên FARC nhận thông tin hoặc thời điểm FARC kích hoạt cảnh báo tự động.

- ΔT_{tn}: Khoảng thời gian từ khi RCT bắt đầu gửi tin báo đến thời điểm thông tin được thông báo cho nhân viên FARC hoặc thời điểm FARC kích hoạt một hành động tự động ($\Delta T_{tn} = T_{tn} - T_{RCT}$)

- $T_{hđ}$: Thời điểm hành động đầu tiên được thực hiện bởi nhân viên FARC hoặc FAMS theo quy trình đã định.

- $\Delta T_{hđ}$: Khoảng thời gian từ khi RCT gửi tin báo đến thời điểm hành động đầu tiên được thực hiện bởi nhân viên FARC hoặc FAMS theo quy trình đã định ($\Delta T_{hđ} = T_{hđ} - T_{RCT}$)

CHÚ THÍCH 1: Việc xử lý tin báo trong RCT quy định tại 5.3 của tiêu chuẩn này. Các mốc thời gian xử lý tin báo trong FATB và FARC tham khảo thêm tại Phụ lục H

CHÚ THÍCH 2: Đối với các tin báo cháy, khi xử lý tự động (không áp dụng lọc tin báo cháy) T_{tn} và ΔT_{tn} có thể bằng với $T_{hđ}$ và $\Delta T_{hđ}$

CHÚ THÍCH 3: Khi có một tin báo cháy được tiếp nhận tại FARC, có thể có nhiều giá trị $T_{hđ}$ ($\Delta T_{hđ}$) tương ứng với các hành động tự động hoặc thủ công khác nhau đầu tiên (ví dụ hành động tự động có thể gồm FAMS tự động gửi tin nhắn hoặc cảnh báo đến cơ sở được giám sát hoặc lực lượng chữa cháy; hoặc nhân viên gọi điện xác minh đến cơ sở được giám sát...), tuy nhiên tất cả các giá trị $T_{hđ}$($\Delta T_{hđ}$) đều phải đáp ứng quy định về hiệu năng xử lý tin nhắn

CHÚ THÍCH 4: Ví dụ về các mốc thời gian (T_{RCT}, T_{FAMS}, T_{tn}, $T_{hđ}$) trong sơ đồ hình 1:

- Lúc 10:03':05" một tin báo cháy được gửi đến RCT. RCT xử lý và bắt đầu gửi tin báo cháy đến FAMS lúc 10:03':05" (T_{RCT})

- FAMS nhận được tin báo cháy lúc 10:03':06" (T_{FAMS})

- FAMS kích hoạt chuông cảnh báo và hiển thị tin báo cháy lên màn hình cho nhân viên vận hành lúc 10:03:08" (T_{tn})

- FAMS gửi email, tin nhắn, cuộc gọi tự động cho chủ cơ sở được giám sát lúc 10:03:10" (T_{tn},$T_{hđ}$)

- Nhân viên vận hành FARC gửi tin báo cháy kèm thông tin cơ sở được giám sát cho lực lượng chữa cháy lúc 10:03':25" ($T_{hđ}$)

6.1.2 Xử lý tin báo cháy.

6.1.2.1 FARC phải có quy trình xử lý tin báo cháy để bảo đảm rằng các tin báo giả được loại bỏ trước khi chuyển đến lực lượng chữa cháy, để đạt được điều này quy trình có thể gồm quá trình lọc tin báo cháy. Quy trình xử lý tin báo cháy phải đáp ứng các yêu cầu sau:

a) được thống nhất với lực lượng chữa cháy;

b) được xây dựng phù hợp với từng loại hình cơ sở được giám sát;

c) được thống nhất với từng cơ sở được giám sát về mức độ chính xác của các tin báo cháy.

CHÚ THÍCH: Các tin báo cháy xuất phát từ một cơ sở được giám sát có thể được chuyển đến lực lượng chữa cháy mà không phải thực hiện quy trình lọc nếu có sự thống nhất giữa cơ sở và FARC rằng mỗi báo cháy xuất phát tại cơ sở là tin báo cháy thực. Để đạt được điều này, một cơ sở có thể áp dụng các phương pháp xác minh báo cháy để tăng xác suất rằng là một báo cháy thực. Các phương pháp xác minh có thể gồm: Xác minh tuần tự (một tin báo cháy được phát ra từ hai hoặc nhiều nguồn phát hiện độc lập và được xem là tin báo cháy thực); xác minh âm thanh, hình ảnh bổ sung; được người có mặt tại hiện trường xác nhận rằng đó là một tin báo cháy thực.

6.1.2.2 Hiệu năng xử lý tin báo cháy

6.1.2.2.1 FARC phải có hiệu năng xử lý tin báo cháy để bảo đảm khoảng thời gian từ khi RCT gửi tin báo cháy đến thời điểm hành động đầu tiên được thực hiện ($\Delta T_{hđ}$) đáp ứng các yêu cầu sau:

a) không quá 30 s đối với 80 % số tin báo cháy nhận được;

b) không quá 60 s đối với 98,5 % số tin báo cháy nhận được.

CHÚ THÍCH: Đối với các tin báo cháy áp dụng quy trình lọc như quy định tại 6.1.2.3, khoảng thời gian trì hoãn do lọc báo cháy có thể không tính vào $\Delta T_{hđ}$ nếu có sự thỏa thuận giữa FARC và cơ sở được giám sát.

6.1.2.2.2 Việc tuân thủ các tiêu chí tại 6.1.2.2.1 phải được đạt được trong khoảng thời gian luân phiên 12 tháng.

6.1.2.3 Lọc tin báo cháy

6.1.2.3.1 Khi quy trình xử lý tin báo tại FARC áp dụng lọc tin báo cháy, FARC phải lập tức chuyển tín hiệu đến lực lượng chữa cháy nếu:

a) Không thể liên hệ với cơ sở được giám sát trong vòng 60 s, hoặc

b) Trong vòng tối đa 90 s, nếu liên lạc với người tại cơ sở được giám sát không thể xác định rõ ràng rằng tín hiệu là cảnh báo giả.

c) Một người tại cơ sở được giám sát xác nhận có cháy.

CHÚ THÍCH 1: Thời gian bắt đầu lọc báo cháy được tính từ thời điểm hành động đầu tiên được thực hiện bởi nhân viên FARC hoặc FAMS theo quy trình đã định ($T_{hđ}$).

CHỨ THÍCH 2: Phụ lục H mô tả sơ đồ logic quá trình lọc tin báo cháy

6.1.2.3.2 Việc áp dụng các quy định lọc tin báo cháy tại 6.1.2.3.1 có thể được điều chỉnh để phù hợp với điều kiện thực tế và yêu cầu vận hành cụ thể, nếu có yêu cầu hoặc chấp thuận từ cơ quan quản lý chuyên ngành về phòng cháy và chữa cháy. Trong trường hợp điều chỉnh, phải thông báo và thống nhất với cơ sở được giám sát.

6.1.3 Hệ thống quản lý tin báo cháy

FAMS trong FARC có nhiệm vụ:

a) Lưu trữ, tổ chức, kiểm soát, điều khiển, quản lý và cho phép truy xuất dữ liệu liên quan của cơ sở được giám sát.

b) Kết nối với RCT để tiếp nhận và hiển thị tự động các tin báo từ mỗi FDAS.

c) Tiếp nhận, phân loại, xử lý và hiển thị các loại tin báo khác từ hệ thống truyền tin báo cháy, bao gồm tin báo trạng thái và tin báo lỗi.

CHÚ THÍCH: Phụ lục I mô tả chi tiết về một hệ thống FAMS điển hình

6.1.4 Đồng bộ hóa thời gian

6.1.4.1 Tất cả các thiết bị của FARC có ghi nhận mốc thời gian phải được đồng bộ với thời gian UTC. Việc đồng bộ có thể được thực hiện tự động bởi FAMS, nhân viên FARC, nguồn đồng bộ nội bộ hoặc bên ngoài FARC.

6.1.4.2 FAMS phải tạo ra cảnh báo lỗi nếu:

a) Hệ thống không đồng bộ hóa trong vòng 24 h, hoặc

b) Chênh lệch thời gian của FAMS so với giờ UTC quá 5 s.

6.1.4.3 Với các thiết bị có giao diện đồ họa người dùng (GUI) để xử lý tin báo, FARC phải luôn hiển thị giờ địa phương đang được sử dụng.

GHI CHÚ: Tại Việt Nam, giờ địa phương đang được sử dụng là UTC+7:00.

6.1.5 Lưu trữ sự kiện

6.1.5.1 FARC phải tự động ghi nhận và lưu trữ các sự kiện sau đây kèm theo dấu thời gian và ngày:

a) T_{RCT}, T_{FAMS}, T_{tn} và $T_{hđ}$;

b) Bất kỳ liên lạc bên ngoài nào mà FARC nhận được và có chứa thông tin nhận dạng của bên liên lạc (ví dụ: Cơ sở được giám sát hoặc cuộc điện thoại gọi đến), bao gồm loại và nội dung của liên lạc;

c) Bất kỳ hành động nào của nhân viên vận hành, bao gồm chi tiết về hành động thực hiện và danh tính của nhân viên vận hành thực hiện và hoàn tất hành động đó; bao gồm dấu thời gian và ngày tại thời điểm hoàn tất hành động;

d) Bất kỳ hành động tự động nào do FAMS tự thực hiện (chi tiết xem Phụ lục I).

6.1.5.2 Tất cả dữ liệu liên quan đến liên lạc và hành động phải được lưu giữ ở định dạng có thể truy xuất trong thời gian tối thiểu ba tháng.

6.1.6 Lưu trữ dữ liệu gốc

6.1.6.1 Dữ liệu gốc của mỗi FDAS kết nối với FARC phải được lưu trữ và dễ dàng truy cập. Dữ liệu gốc bao gồm:

a) Số tham chiếu FDAS duy nhất;

b) Tên, địa chỉ, số điện thoại của cơ sở được giám sát;

c) Các hành động cần thực hiện đối với mỗi loại tin báo;

d) Thông tin liên hệ của lực lượng chữa cháy, chủ hoặc người đại diện cơ sở được giám sát hoặc các đối tượng khác có liên quan;

đ) Bất kỳ dữ liệu cụ thể nào khác cần thiết để FARC xử lý các tin báo cháy, báo lỗi và thực hiện các hành động đã thỏa thuận;

e) Định nghĩa mức độ ưu tiên của các loại tin báo và thời gian phản hồi liên quan (nếu khác với hiệu năng mặc định đã được quy định ở trên).

6.1.6.2 Dữ liệu gốc phải luôn được cập nhật phù hợp với thực tế. Mọi thay đổi trong dữ liệu gốc phải được ghi lại với dấu thời gian và ngày.

6.1.6.3 Dữ liệu gốc thay đổi do thay đổi của cơ sở được giám sát phải được lưu trữ trong thời gian tối thiểu 3 năm.

6.2 Quy trình vận hành

6.2.1 FARC phải xây dựng quy trình vận hành và duy trì việc thực hiện quy trình này.

6.2.2 Quy trình vận hành FARC phải đáp ứng các yêu cầu sau:

a) Xác định rõ người chịu trách nhiệm xây dựng, triển khai, thực hiện quy trình, đánh giá và duy trì quy trình.

b) Ngày phát hành chính thức;

c) Được cung cấp cho toàn bộ nhân viên theo yêu cầu nhiệm vụ của họ;

d) Được lập thành tài liệu cho các nội dung quy định tại Phụ lục K.

6.3 Cung cấp điện cho trung tâm tiếp nhận

6.3.1 FARC phải được cấp điện từ 2 nguồn độc lập bao gồm nguồn điện chính và nguồn dự phòng.

6.3.2 Khu vực vận hành FARC phải có chỉ báo về nguồn điện hiện tại đang được sử dụng. Nếu nguồn điện chính bị mất, phải có cảnh báo bằng âm thanh hoặc hình ảnh được kích hoạt đủ để cảnh báo nhân viên vận hành.

6.3.3 Chuyển đổi giữa nguồn điện chính và nguồn điện dự phòng không được làm gián đoạn hoạt động bình thường của các thiết bị.

6.3.4 Khi nguồn điện chính được khôi phục, các thiết bị của FARC phải được tự động chuyển về cấp nguồn bằng nguồn điện chính.

6.3.5 Nguồn điện chính phải đáp ứng các điều kiện sau:

a) Được lấy từ nguồn điện lưới hoặc một nguồn điện bảo đảm độ tin cậy cung cấp điện tương tự;

b) Đáp ứng đủ công suất cho tất cả các thiết bị điện của FARC hoạt động bình thường, không gián đoạn và đồng thời sạc lại cho các thiết bị lưu trữ năng lượng dự phòng đến dung lượng yêu cầu trong

vòng 24h;

6.3.6 Nguồn điện dự phòng phải đáp ứng các yêu cầu sau:

a) Đảm bảo hoạt động cho các thiết bị điện thiết yếu trong tối thiểu 24h.

b) Công suất tính toán của nguồn dự phòng phải ≥ 1,2 lần tổng công suất tối đa của các thiết bị điện thiết yếu.

CHÚ THÍCH: Các thiết bị điện thiết yếu là các thiết bị điện phục vụ FARC hoạt động an toàn và duy trì các yêu cầu của tiêu chuẩn này. Ví dụ gồm: Các thiết bị duy trì hoạt động giám sát, tiếp nhận tin báo cháy hoặc báo lỗi (thiết bị truyền tin, thiết bị mạng có liên quan, FAMS ...); các thiết bị phòng cháy, chữa cháy trang bị, lắp đặt tại FARC; các thiết bị bảo đảm an ninh, an toàn của FARC...

7 Kiểm tra, thử nghiệm

7.1 Kiểm tra hiệu năng của FATSN

7.1.1 Quy định chung

7.1.1.1 Mục tiêu của việc kiểm tra hiệu năng của FATB nhằm đảm bảo rằng tất cả các thành phần trong hệ thống được giám sát hiệu quả, đồng thời có khả năng phát hiện, tạo ra và truyền thành công các tín hiệu lỗi khi xảy ra sự cố. FATSP phải duy trì việc kiểm tra hiệu năng của FATB theo quy định.

7.1.1.2 Việc kiểm tra hiệu năng của FATB bao gồm:

a) Kiểm tra để xác minh rằng chức năng của hệ thống tuân thủ các yêu cầu tại tiêu chuẩn này và các tiêu chuẩn hiện hành có liên quan, bao gồm các thử nghiệm để xác nhận khả năng truyền tin và giám sát tình trạng của FATB;

b) Kiểm tra thường xuyên hoặc định kỳ để xác nhận độ khả dụng của FATB.

CHÚ THÍCH: Việc thử nghiệm giao diện SPT và FDAS được thực hiện theo 7.2 của tiêu chuẩn này.

7.1.2 Hiệu năng của FATSN

7.1.2.1 Trong trường hợp mà các FDAS tạo thành các nhóm riêng biệt về mặt địa lý và các nhóm này kết nối tới một RCT riêng biệt trong FARC hoặc có thể được xác định riêng biệt theo phương pháp khác thì mỗi nhóm có thể được xem là một FATSN độc lập. Khi sử dụng phương pháp phân nhóm này, việc kiểm tra sẽ được thực hiện riêng biệt trên từng nhóm đã xác định. FATSP phải lập tài liệu về các tiêu chí sử dụng để phân chia FATB thành các FATSN.

7.1.2.2 Việc xác minh hiệu năng của từng FATSN phải đảm bảo rằng với cấu hình hệ thống và số lượng FDAS được kết nối dự kiến, từng FATSN có khả năng đáp ứng các yêu cầu tại 5.1.2. Việc này được thực hiện thông qua kiểm tra hiệu năng của các FATB đã được đưa vào vận hành thực tế.

7.1.3 Thời gian truyền

7.1.3.1 FATB phải được kiểm tra để xác nhận khả năng truyền tin chính xác, bao gồm cả các tin báo liên quan đến giám sát trạng thái của hệ thống. Thời gian truyền một tín hiệu báo cháy, báo lỗi hoặc một tín hiệu giả lập tín hiệu báo cháy, báo lỗi để kiểm tra hiệu năng của FATB phải đáp ứng quy định tại 5.1.3.2

7.1.3.2 Thời gian báo cáo lỗi phải đáp ứng yêu cầu tại Bảng 1.

7.1.4 Tần suất kiểm tra hiệu năng

7.1.4.1 Việc kiểm tra hiệu năng của FATB theo quy định tại 5.1.3 phải được thực hiện định kỳ và bắt buộc trong các trường hợp sau:

a) khi đưa FATB vào vận hành lần đầu;

b) sau bất kỳ thay đổi cấu hình nào của FATB (thay đổi SPT, RCT và/hoặc mạng truyền dẫn).

7.1.4.2 Trong trường hợp số lượng tin báo truyền qua hệ thống thay đổi theo thời gian hoặc khi FATP của FATB đồng thời được sử dụng bởi ứng dụng khác làm ảnh hưởng tới tốc độ truyền theo thời gian, thì việc kiểm tra hiệu năng của hệ thống phải phản ánh đúng thời điểm tin báo thường xảy ra và khi lưu lượng truyền tải dữ liệu mạng truyền dẫn đạt cao nhất.

CHÚ THÍCH 1: Số lượng bản tin truyền qua hệ thống có thể thay đổi theo thời điểm trong năm; ví dụ, vào mùa hè, nguy cơ cháy cao khiến số lượng tin báo cháy tăng so với các mùa khác. Vì vậy, việc kiểm tra hiệu năng của hệ thống cần được thực hiện vào giai đoạn cao điểm này.

CHÚ THÍCH 2: Khi FATP của FATB chia sẻ băng thông với các ứng dụng khác (xem 5.1.2), thì vào giờ cao điểm sử dụng các ứng dụng đó (ví dụ: giờ hành chính), băng thông sẵn có cho truyền tin báo cháy có thể bị suy giảm. Do đó, việc kiểm tra hiệu năng của hệ thống nên được thực hiện vào các thời điểm cao điểm này để phản ánh điều kiện vận hành thực tế.

7.1.4.3 Kết quả kiểm tra hiệu năng của từng FATB và FATSN phải được tổng hợp, phân tích và đánh giá từng chu kỳ liên tục kéo dài 3 tháng. Tuy nhiên, nếu một hệ thống tạm thời không hoạt động hoặc

không phát sinh tín hiệu cần kiểm tra trong khoảng thời gian này, thì không bắt buộc phải thực hiện kiểm tra trong chu kỳ đó.

7.1.5 Độ khả dụng

7.1.5.1 Hồ sơ

7.1.5.1.1 Tất cả các lỗi và các lần kiểm tra hiệu năng của mọi FATB và FATSN phải được ghi nhận và lưu trữ có hệ thống bởi FATSP.

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

7.1.5.1.3 Thông tin cần lưu trữ cho mỗi lỗi của FATB bao gồm:

a) thời gian và ngày lỗi được phát hiện,

b) thời gian và ngày hệ thống được khôi phục hoạt động bình thường sau khi xử lý lỗi.

7.1.5.1.4 Hồ sơ phải được lưu giữ trong thời gian tối thiểu 3 năm.

7.1.5.1.5 Hồ sơ về độ khả dụng của FATB và FATSN phải được cung cấp cho các bên liên quan (ví dụ: khách hàng, FARC, đơn vị lắp đặt, người dùng cuối, tổ chức chứng nhận, cơ quan quản lý...).

7.1.5.1.6 Phải có khả năng truy vết các lỗi riêng lẻ của FATP và FATB trong dữ liệu tổng hợp để phục vụ phân tích lỗi và xác định thời điểm khắc phục

7.1.5.2 Tính toán

7.1.5.2.1 Tổng quan

Hồ sơ ghi nhận về tất cả các lần kiểm tra hiệu năng sẽ được sử dụng để xác định độ khả dụng tương ứng của từng hệ thống FATB hoặc FATSN

7.1.5.2.2 Tính toán độ khả dụng của FATB

Mỗi lần một FATB không khả dụng (xem 5.1.7.3), thời gian gián đoạn hoạt động của FATB đó sẽ được xác định. Đối với mỗi chu kỳ bảy ngày, độ khả dụng của FATB sẽ được tính như sau:

$$WA = \left(1 - \frac{WF}{10\,080}\right) \times 100\% \quad (1)$$

Trong đó:

WA: Độ khả dụng tính theo tuần của FATB, biểu thị theo phần trăm;

WF: Tổng thời gian lỗi của FATB trong khoảng thời gian bảy ngày, tính theo phút như quy định tại 5.1.7.4.

CHÚ THÍCH: 10 080 = 7 ngày x 24h x 60min, là số phút trong một tuần.

7.1.5.2.3 Tính toán khả dụng của FATSN

a) Thời gian lỗi của một lần lỗi FATSN được xác định theo công thức:

$$FT = DF \times NA \quad (2)$$

Trong đó:

FT: Thời gian lỗi của một lần sự cố lỗi đơn lẻ trong FATSN, được biểu thị bằng phút;

DF: Thời gian lỗi của một FATB, tính theo phút như quy định tại 5.1.7.4

NA: số FDAS bị ảnh hưởng bởi lỗi

b) Xác định tổng thời gian lỗi hàng năm của FATSN theo công thức:

$$FY = \sum_{i=1}^{n} FT_i \quad (3)$$

Trong đó:

FT_i: Thời gian lỗi của một lỗi bất kỳ thứ i trong tổng số n lỗi trong năm của FATSN. FT_i được tính theo công thức (2).

c) Xác định độ khả dụng của FATSN theo công thức

$$YA = \left(1 - \frac{YF}{525\,600 \times NC}\right) \times 100\% \quad (4)$$

Trong đó:

YA: Độ khả dụng trong một năm của FATSN, biểu thị theo phần trăm.

YF: Tổng thời gian lỗi hàng năm của FATSN, được thể hiện bằng phút. YF được tính theo công thức (3)

NC: Tổng số FDAS được kết nối.

CHÚ THÍCH: 525 600 = 365 ngày x 24 h x 60 min, là số phút trong một năm

7.1.5.2.4 Tổng thời gian lỗi phải bao gồm tất cả các lỗi trong năm, kể cả các lỗi đã được khắc phục. Số lượng FATB sử dụng để tính toán độ khả dụng của FATSN được xác định tại thời điểm 24h:00 của ngày cuối cùng của năm tính toán. Độ khả dụng hàng năm của hệ thống được xác định bằng trung bình số học của độ khả dụng hàng tuần trong 52 tuần liên tiếp của cùng năm.

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 FATB sẽ được ghi nhận vào cuối ngày 31 tháng 12 năm 2025 (24h:00 ngày 31 tháng 12 năm 2025). Độ khả dụng của hệ thống trong năm 2025 sẽ là trung bình số học của độ khả dụng hàng tuần trong 52 tuần của năm 2025.

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

CHÚ THÍCH: Khi hệ thống tăng hoặc giảm FATB, 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.

7.1.5.2.6 Tính toán độ khả dụng phải được thực hiện chính xác tối thiểu đến hai chữ số sau dấu phẩy thập phân. Việc tính toán và kết phải được lưu giữ trong thời gian tối thiểu 3 năm.

7.2 Kiểm tra, thử nghiệm SPT

7.2.1 Yêu cầu chung

7.2.1.1 Các điều kiện môi trường

Trừ khi có quy định khác trong một quy trình thử nghiệm cụ thể (ví dụ như các thử nghiệm môi trường), thì phép thử phải được thực hiện sau khi mẫu thử đã được ổn định trong các điều kiện môi trường tiêu chuẩn dành cho thử nghiệm như quy định tại 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 có sai lệch về các thông số có thể làm ảnh hưởng đến kết quả đo, thì những sai lệch đó phải được giữ ở mức tối thiểu trong suốt toàn bộ thời gian thực hiện các phép đo là một phần của chương trình thử nghiệm.

7.2.1.2 Chuẩn bị mẫu thử

7.2.1.2.1 Cấu hình của mẫu thử

a) Cấu hình mẫu thử ít nhất phải đầy đủ các loại SPT và các thành phần liên quan. Báo cáo thử nghiệm phải nêu rõ đặc điểm chi tiết của SPT được sử dụng.

b) Các thành phần khác trong FATB như FDAS, mạng và RCT có thể được cung cấp dưới dạng thiết bị mô phỏng và/hoặc mạng mô phỏng. Trong trường hợp sử dụng RCT (hoặc RCT mô phỏng) cho các thử nghiệm, RCT đó phải đáp ứng yêu cầu tại 5.1 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 SPT.

7.2.1.2.2 Bố trí lắp đặt

Mẫu thử nghiệm phải được lắp đặt theo hướng sử dụng thông thường, bằng các chi tiết gắn phù hợp với hướng dẫn của nhà sản xuất SPT. 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.

7.2.1.2.3 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 quy định khác, nguồn cấp điện phải ở trạng thái danh định.

c) Tất cả các mạch tín hiệu, mạch đầu ra, và các giao diện mạng truyền dẫn của SPT phải được kết nối dây dẫn và thiết bị tương ứng hoặc tải giả lập. Ít nhất một mạch của mỗi loại phải được thử với tải lớn nhất trong phạm vi hoạt động mà nhà sản xuất SPT quy định.

7.2.2 Chương trình thử nghiệm và số lượng mẫu thử.

7.2.2.1 Chương trình thử nghiệm bao gồm các thử nghiệm chức năng trong điều kiện môi trường quy định tại 7.2.1.1 kết hợp với 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.

CHÚ THÍCH: Đối với từng mẫu thử, thử nghiệm chức năng sau một thử nghiệm môi trường có thể được coi là thực hiện thử nghiệm chức năng trước và thử nghiệm môi trường kế tiếp (xem 7.2.2.4).

7.2.2.2 Thử nghiệm chức năng

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

Bảng 5 - Các thử nghiệm chức năng của SPT

Mục	Yêu cầu kiểm tra	Mục tiêu kiểm tra/đánh giá	Phương pháp
5.2.1.1; 5.2.1.2; 5.2.1.3; 5.2.1.6, 5.2.2.6	Hoạt động của SPT	Chứng minh SPT có khả năng tiếp nhận, chuyển tiếp tin báo, chỉ báo trạng thái và tạo ra các tin báo lỗi theo yêu cầu.	Kiểm tra (mục E.1.1 Phụ lục E)
5.2.1.4 và phụ lục G	Giao diện với FDAS (nối tiếp)	Chứng minh giao diện nối tiếp với FDAS phù hợp với tài liệu của nhà sản xuất.	Xác thực (mục E.1.2.1 Phụ lục E)
	Giao diện với FDAS (song song)	Chứng minh giao diện song song với FDAS tuân thủ 5.2.1.4 và Phụ lục G.	Kiểm tra (mục E.1.2.2 Phụ lục E)
	Giao diện với FDAS (độc quyền)	Chứng minh giao diện độc quyền với FDAS phù hợp với tài liệu của nhà sản xuất.	Xác thực (mục E.1.2.3 Phụ lục E)
5.2.1.5	Giám sát giao diện mạng truyền dẫn	Chứng minh SPT có thể phát hiện lỗi FATP khi mỗi giao diện mạng truyền dẫn bị lỗi.	Kiểm tra (mục E.1.3 Phụ lục E)
5.2.1.7 và phụ lục D	Mức độ truy cập	Chứng minh tất cả các mức truy cập đều được thiết lập và hoạt động đúng yêu cầu.	Kiểm tra (mục E.1.4 Phụ lục E)
5.2.1.8	Bảo mật chống giả mạo và bảo mật thông tin	Xác minh tài liệu công bố của nhà sản xuất về cơ chế chống giả mạo và bảo mật thông tin.	Xác thực (mục E.1.5 Phụ lục E)
5.2.1.10	Tải lên và tải xuống phần mềm và chương trình cơ sở	Chứng minh SPT có thể phục hồi hoạt động sau khi tải lên hoặc tải xuống phần mềm và chương trình cơ sở không thành công.	Kiểm tra (mục E.1.6 Phụ lục E)
5.2.1.11	Lưu trữ tham số	Chứng minh bộ nhớ cấu hình của SPT không bị ảnh hưởng bởi mất điện hoặc khởi động lại.	Kiểm tra (mục E.1.7 Phụ lục E)
5.2.1.12	Bảo vệ nhật ký	Chứng minh sự tuân thủ theo tài liệu của nhà sản xuất SPT rằng nhật ký được bảo vệ khỏi sự thay đổi hoặc xóa trái phép.	Xác thực (mục E.1.9 Phụ lục E)
	Khả năng lưu trữ và thời gian lưu trữ của nhật ký	Chứng minh nhật ký có thể lưu và giữ được số lượng sự kiện theo yêu cầu.	Kiểm tra (mục E.1.10 Phụ lục E)
	Độ phân giải dấu thời gian	Chứng minh dấu thời gian kèm theo sự kiện tuân thủ quy định tại 5.2.1.12	Kiểm tra (mục E.1.11 Phụ lục E)
	Ghi nhật ký sự kiện	Chứng minh nhật ký ghi lại được các sự kiện theo quy định tại Bảng 2.	Kiểm tra (mục E.1.8 Phụ lục E)
5.2.2.2	Tài liệu	Kiểm tra tài liệu của nhà sản xuất SPT theo yêu cầu của 5.2.2.2.	Xác thực (mục E.1.12 Phụ lục E)
5.2.2.2	Phương pháp xác định hiệu năng	Chứng minh phương pháp được nêu trong tài liệu của nhà sản xuất có thể được sử dụng để xác định hiệu năng của FATB	Xác thực (mục E.1.13 Phụ lục E)
Kiểm tra: Là việc thử nghiệm, vận hành thực tế để đánh giá mức độ đáp ứng với yêu cầu tại tiêu chuẩn; Xác thực: Là việc xem xét tài liệu của nhà sản xuất để xác định mức độ phù hợp với yêu cầu tại tiêu chuẩn.			

7.2.2.3 Thử nghiệm môi trường

7.2.2.3.1 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.

7.2.2.3.2 Các chương trình thử nghiệm môi trường của SPT được tóm tắt tại Bảng 6, quy định tại Phụ lục E

Bảng 6 - Tóm tắt các thử nghiệm môi trường của SPT

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

7.2.2.4 Số lượng mẫu thử

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

7.2.2.4.2 Nếu cung cấp nhiều mẫu để thử nghiệm môi trường, các phép thử có thể được phân chia giữa các mẫu này và trình tự thực hiện các phép thử có thể được sắp xếp linh hoạt, miễn là đảm bảo mỗi phép thử đều được thực hiện đầy đủ, và các phép thử chức năng bắt buộc phải được thực hiện trước và sau từng phép thử môi trường.

CHÚ THÍCH:

Ví dụ 1. Nếu có 2 mẫu được cung cấp để làm thử nghiệm về môi trường, thì các thử nghiệm về vận hành (E.2.1 đến E.2.6 phụ lục E) có thể được thử nghiệm 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 bất kỳ trong số các phép thử về độ bền (E.2.7, E.2.8 phụ lục E). Các phép thử 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 trong số các phép thử về độ bền. Phép thử về độ bền khác còn lại 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.

7.3 Kiểm tra, thử nghiệm RCT

7.3.1 Chuẩn bị thử nghiệm

7.3.1.1 Điều kiện thử nghiệm

Tất cả các phép thử phải được tiến hành trong điều kiện môi trường tiêu chuẩn, trừ khi có quy định cụ thể khác trong từng phép thử. Các điều kiện môi trường tiêu chuẩn như sau:

Nhiệt độ: 15 °C đến 35 °C;

Độ ẩm tương đối: 25 % đến 75 %;

Áp suất khí quyển: 86 kPa đến 106 kPa.

7.3.1.2 Lắp đặt

RCT phải được lắp đặt theo hướng dẫn của nhà sản xuất. Bất kỳ thiết bị bổ sung cần thiết để thực hiện các thử nghiệm (ví dụ mô phỏng FATB và SPT) sẽ do nhà sản xuất RCT cung cấp trên cơ sở thỏa thuận với đơn vị thử nghiệm.

7.3.1.3 Nguồn điện cấp

Nguồn điện cung cấp cho RCT phải đáp ứng yêu cầu kỹ thuật theo quy định của nhà sản xuất RCT.

7.3.2 Yêu cầu chung

7.3.2.1 Các thử nghiệm chức năng nhằm chứng minh rằng RCT có khả năng thực hiện đầy đủ các chức năng cần thiết theo quy định của tiêu chuẩn này. Nhà sản xuất RCT phải cung cấp một cấu hình thử nghiệm hoàn chỉnh, có khả năng đánh giá toàn diện, đầy đủ các chức năng bắt buộc của RCT. Cấu hình này có thể bao gồm các thiết bị mô phỏng FDAS, SPT và/hoặc mô hình mạng giả lập nhằm

thay thế cho hệ thống thực tế khi cần thiết.

7.3.2.2 Từng FATP riêng lẻ sẽ phải kiểm tra về thời gian báo cáo lỗi tối đa theo quy định của tiêu chuẩn này.

7.3.2.3 Tất cả các giao diện mạng mà RCT sử dụng để truyền và nhận tín hiệu, cũng như giao diện kết nối với FAMS phải được kiểm tra để bảo đảm rằng RCT có thể giao tiếp với hệ thống một cách hiệu quả.

7.3.2.4 Các thử nghiệm được tóm tắt tại Bảng 7, quy định tại Phụ lục F.

Bảng 7 - Tóm tắt các thử nghiệm chức năng của RCT

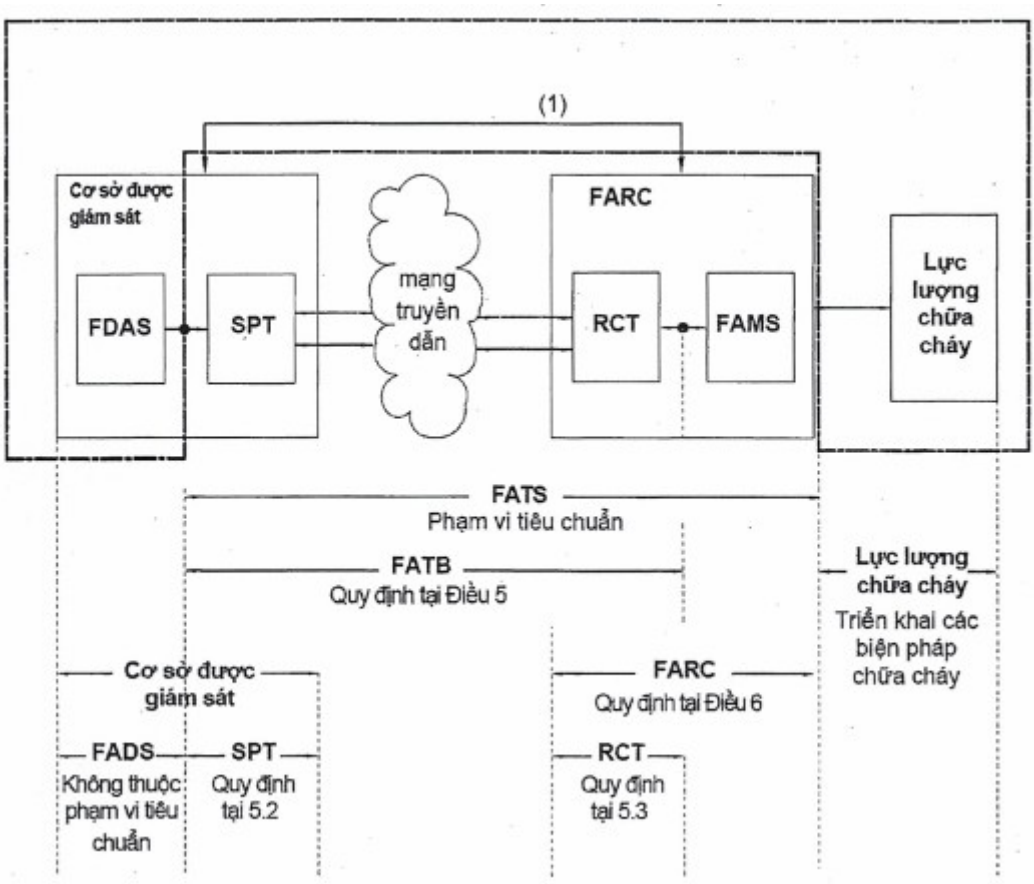
Mục	Yêu cầu kiểm tra	Mục tiêu kiểm tra/đánh giá	Phương pháp
5.3.1	Xử lý tin báo	Chứng minh khả năng của RCT trong việc nhận, xử lý và chuyển tiếp tin báo.	Kiểm tra (mục F.7. Phụ lục F)
5.3.2 và Phụ lục D	Cấp quyền truy cập	Chứng minh tất cả các mức truy cập đều được thiết lập và hoạt động đúng yêu cầu.	Kiểm tra (mục F.1. Phụ lục F)
5.3.3	Tải lên và tải xuống phần mềm	Chứng minh RCT có thể phục hồi hoạt động sau khi tải lên hoặc tải xuống phần mềm không thành công.	Kiểm tra (mục F.2. Phụ lục F)
5.3.4	Lưu trữ tham số cấu hình và dữ liệu đặc thù của người dùng.	Chứng minh RCT không mất bất kỳ tham số cấu hình hoặc dữ liệu người dùng nào sau khi khởi động lại hoặc mất điện.	Kiểm tra (mục F.3. Phụ lục F)
5.3.5	Giám sát và thông báo lỗi	Chứng minh RCT có thể phát hiện và báo lỗi FATB tới FAMS.	Kiểm tra (mục F.4. Phụ lục F)
5.3.6	Giao diện với FAMS	Chứng minh giao diện với FAMS được giám sát đúng yêu cầu.	Kiểm tra (mục F.5. Phụ lục F)
5.3.7	Tín hiệu lỗi	Chứng minh RCT có khả năng phát hiện và báo lỗi theo yêu cầu.	Kiểm tra (mục F.6. Phụ lục F)
5.3.8	Ghi nhật ký sự kiện	Chứng minh tất cả các sự kiện bắt buộc được ghi lại theo yêu cầu trong Bảng 4.	Kiểm tra (mục F.8. Phụ lục F)
	Độ phân giải và đồng bộ hóa thời gian	Chứng minh dấu thời gian kèm theo sự kiện đáp ứng yêu cầu.	Kiểm tra (mục F.9. Phụ lục F)
	Thơi gian lưu giữ của nhật ký	Chứng minh tài liệu của nhà sản xuất RCT cung cấp có quy định rõ ràng về thời gian lưu giữ tối thiểu là 3 năm.	Xác thực (mục F.10. Phụ lục F)
	Phương pháp tối ưu hóa lưu trữ sự kiện (nếu có)	Chứng minh việc lưu trữ sự kiện theo nhóm được thực hiện đúng như quy định tại 5.3.8.	Kiểm tra (mục F.11. Phụ lục F)
	Nhận dạng người dùng trong nhật ký	Chứng minh nhận dạng người dùng được ghi được ghi nhận đúng với các sự kiện theo quy định tại Bảng 4.	Kiểm tra (mục F.12. Phụ lục F)
5.3.9	Chế độ vận hành	Chứng minh rằng các chế độ vận hành được thực hiện đúng yêu cầu.	Kiểm tra (mục F.13. Phụ lục F)
5.3.10	Tấn công từ chối dịch vụ	Chứng minh tài liệu của nhà sản xuất RCT mô tả rõ khả năng chống lại tấn công từ chối dịch vụ.	Xác thực (mục F.14. Phụ lục F)
5.3.11	Bảo mật thông tin	Chứng minh cơ chế bảo mật của RCT đảm bảo an toàn dữ liệu truyền trong FATB.	Xác thực (mục F.15. Phụ lục F)
5.3.12	Bảo mật chống giả mạo	Chứng minh cơ chế bảo vệ RCT chống bị thay thế hoặc giả mạo được thực hiện đầy đủ theo yêu cầu.	Xác thực (mục F.15. Phụ lục F)
5.3.13	Dự phòng RCT	Chứng minh nếu một RCT gặp lỗi không ảnh hưởng đến FATB.	Kiểm tra (mục F.16. Phụ lục F)
5.3.14	Tài liệu	Chứng minh tài liệu của nhà sản xuất đáp ứng yêu cầu tại 5.3.14.	Xác thực (mục F.17. Phụ lục F)
5.3.15	Ghi nhãn	Chứng minh nhãn hiệu và mã thiết bị đáp ứng yêu cầu tại 5.3.15.	Xác thực
CHÚ THÍCH:			

Kiểm tra: Là việc thử nghiệm, vận hành thực tế để đánh giá mức độ đáp ứng với yêu cầu tại tiêu chuẩn; Xác thực: Là việc xem xét tài liệu của nhà sản xuất để xác định mức độ phù hợp với yêu cầu tại tiêu chuẩn.

Phụ lục A

(Tham khảo)

Cấu trúc hệ thống truyền tin báo cháy



CHÚ DẪN:

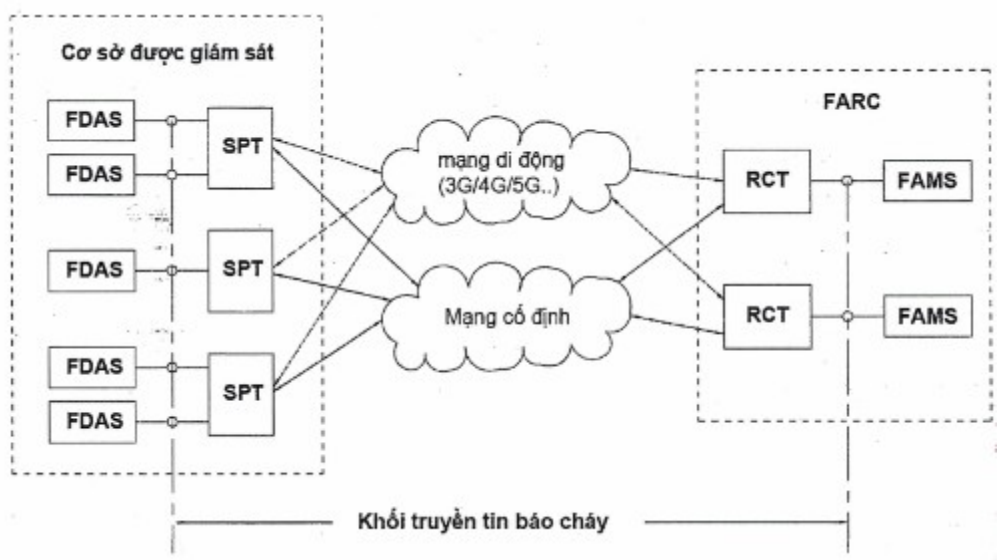
FDAS	Hệ thống báo cháy	**SPT**	Thiết bị truyền, tin báo cháy
FATS	Hệ thống truyền tin báo cháy	**RCT**	Bộ phận tiếp nhận tin báo cháy
FATB	Khối truyền tin báo cháy	**FAMS**	Hệ thống quản lý tin báo cháy
FARC	Trung tâm tiếp nhận báo cháy		
— · — · —	Ngoài phạm vi tiêu chuẩn này		
(1)	Liên hệ, xác minh thông tin báo cháy giữa Trung tâm tiếp nhận báo cháy và cơ sở được giám sát (có thể có hoặc không)		

Hình A.1 - Cấu trúc hệ thống truyền tin báo cháy

Phụ lục B

(Tham khảo)

Cấu trúc khối truyền tin báo cháy



CHÚ DẪN:

⟷	Đường truyền tin báo cháy chính
⟷ (nét đứt)	Đường truyền tin báo cháy dự phòng
FDAS	Hệ thống báo cháy
SPT	Thiết bị truyền tin báo cháy
RCT	Bộ phận tiếp nhận tin báo cháy
FAMS	Hệ thống quản lý tin báo cháy
FARC	Trung tâm tiếp nhận báo cháy

Hình B.1 - Cấu trúc khối truyền tin báo cháy

Phụ lục C

(Tham khảo)

Độ khả dụng

C.1 Tổng quan

C.1.1 FATSP chịu trách nhiệm đo lường và báo cáo độ khả dụng của FATB và FATSN theo định nghĩa tại 3.1.1.2 và 3.1.1.3. Độ khả dụng là tỷ lệ phần trăm thời gian mà FATB hoạt động đáp ứng các yêu cầu của tiêu chuẩn này. Đây là chỉ số hiệu năng quan trọng đánh giá chất lượng của FATB.

C.1.2 Nếu một FATB hoặc FATP hoạt động đảm bảo liên tục và đầy đủ trong tuần, độ khả dụng của nó sẽ là 100 %, nếu không hoạt động trong toàn bộ thời gian thì độ khả dụng là 0 %. Độ khả dụng 99,8 % nghĩa là có 0,2 % không khả dụng, tương đương không hoạt động 20,16 phút trong bảy ngày.

C.1.3 Có mối liên hệ trực tiếp giữa FATB và độ khả dụng của FATSN.

Ví dụ 1: Nếu một FATSN trong một tuần có sự cố mất điện kéo dài 20 phút ảnh hưởng đến 10 % tất cả các FATB, thì độ khả dụng tổng thể của FATSN là 99,989 %. Điều này cho thấy yêu cầu về độ khả dụng của FATSN thường cao hơn đáng kể so với yêu cầu độ khả dụng của từng FATB riêng lẻ.

Ví dụ 2: Sự cố mất điện ảnh hưởng đến kết nối của tất cả các FDAS tại cơ sở trong một năm là 17h, sẽ dẫn đến độ khả dụng của FATSN giảm xuống còn 99,8 %

C.1.4 Độ khả dụng của FATB theo tiêu chuẩn này khác với cách định nghĩa độ khả dụng thường dùng trong lĩnh vực mạng viễn thông. Độ khả dụng của FATB trong tiêu chuẩn được hiểu là khả năng đầu cuối của FATB, bao gồm từ FDAS đến FAMS. Trong khi đó, độ khả dụng của mạng thường không tính đến các thời gian gián đoạn do bảo trì định kỳ hoặc đột xuất và chỉ phản ánh hiệu năng của mạng.

C.2 Độ khả dụng của FATB

C.2.1 Khi một FATP của FATB bị lỗi hoàn toàn nhưng FATP còn lại vẫn duy trì hoạt động bình thường, FATB vẫn được xem là khả dụng. Tuy nhiên, trong trường hợp này, nếu một FATP vẫn tiếp tục lỗi, FATB sẽ hoạt động với FATP còn lại và bất kỳ lỗi nào xảy ra trên FATP này lại sẽ khiến hệ thống mất kết nối hoàn toàn và làm giảm độ khả dụng xuống dưới 100 %.

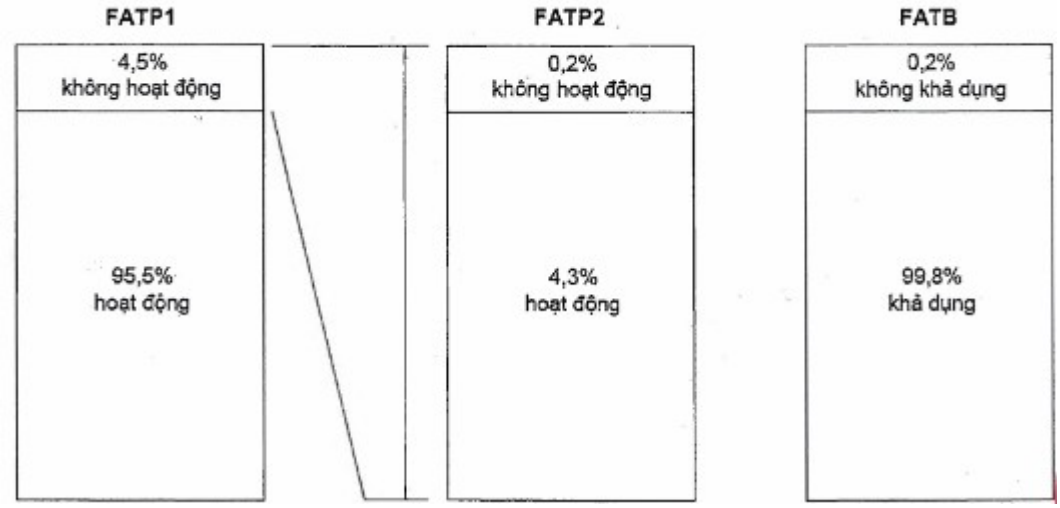
C.2.2 Mục tiêu độ khả dụng của FATB là 99,8 % trong khoảng thời gian một tuần. Một tuần có 168h

nên thời gian ngừng hoạt động tối đa cho phép của FATB là 20 phút. Để đạt được mục tiêu này, cần lựa chọn loại công nghệ truyền dẫn phù hợp và đánh giá kỹ lưỡng môi trường lắp đặt, khoảng cách ước tính từ cơ sở đến thiết bị chuyển mạch hoặc trạm phát sóng cũng như các thỏa thuận dịch vụ rõ ràng về thời gian khôi phục.

C.2.3 Trong tiêu chuẩn này, FATB là loại đường dẫn kép, do đó độ khả dụng của từng đường dẫn riêng lẻ có thể thấp hơn so với độ khả dụng của FATB, miễn là tổ hợp hai đường dẫn vẫn đáp ứng mục tiêu độ khả dụng tổng thể. Minh họa phương pháp để FATB đạt độ khả dụng 99,8 % được trình bày tại C.2.4

C.2.4 Ví dụ về cách đạt được độ khả dụng của FATB là 99,8 %, được minh họa ở hình C.1

Giả sử FATP1 khả dụng 95,5 % và không khả dụng (tình trạng lỗi) 4,5 % trong một tuần. Trong toàn bộ khoảng thời gian 4,5 % khi FATP1 gặp lỗi, FATP2 vẫn duy trì hoạt động với độ khả dụng ở mức 95,5 % và không khả dụng 4,5 %. Khi kết hợp sử dụng cả hai FATP, khả năng mà cả hai đều không hoạt động cùng lúc là (4,5 % x 4,5 % = 0,2025 %), và do đó độ khả dụng tổng thể là 99,8 %.



Hình C.1 - Minh họa về độ khả dụng của khối truyền tin báo cháy

Phụ lục D

(Quy định)

Mức truy cập

Tiêu chuẩn này xác định bốn mức truy cập, được phân loại dựa trên mức độ cho phép người dùng truy cập vào chức năng logic (phần mềm, hệ thống) và vật lý (thiết bị, phần cứng) của hệ thống, thiết bị. Các mức truy cập được thiết lập nhằm bảo đảm an toàn, tính toàn vẹn và khả năng kiểm soát truy cập theo vai trò người dùng.

D.1 Mức truy cập 1: Truy cập cơ bản.

Truy cập logic bao gồm quyền xem các thông tin của chỉ báo trạng thái cơ bản của hệ thống (tín hiệu hoạt động, cảnh báo...), không cho phép thực hiện 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 (tin báo cháy, báo lỗi...).

D.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 kiểm soát bằng các công cụ bảo vệ đơn giản như: Khóa cơ, thẻ truy cập, bàn phím và mã số, mã truy cập.

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

D.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, truy xuất nhật ký và các dữ liệu riêng cụ thể.

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

cập logic mức truy cập 3.

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

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

Truy cập logic bao gồm truy cập để cập nhật phần mềm hệ thống, truy cập để xem các tham số quan trọng chỉ đọc.

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

Người dùng dự kiến ở mức truy cập này có thể là kỹ thuật viên được nhà sản xuất ủy quyền, có thẩm quyền thực hiện cập nhật phần mềm, khắc phục lỗi phần mềm và triển khai các biện pháp bảo mật hệ thống.

Phụ lục E

(Quy định)

Kiểm tra, thử nghiệm thiết bị truyền tin báo cháy

E.1 Kiểm tra chức năng

E.1.1 hoạt động của SPT

E.1.1.1 Mục đích

Thử nghiệm nhằm chứng minh khả năng của SPT đáp ứng quy định tại 5.2.1.1; 5.2.1.2; 5.2.1.3; 5.2.1.6 và 5.2.2.6 trong việc tiếp nhận, chuyển tiếp tín hiệu, chỉ báo trạng thái và tạo tin báo lỗi.

E.1.1.2 Nguyên tắc

Thử nghiệm bao gồm việc tạo ra các tin báo quy định tại 5.2.1.1.1, sau đó xem xét chúng có được SPT tiếp nhận, tạo ra tin báo, chỉ báo trạng thái và truyền tới RCT một cách phù hợp.

Bảng E.1 - Thử nghiệm hoạt động của SPT

Bước	Điều kiện thử	Quy trình thử	Phép đo	Tiêu chí đạt
1.	- FATB được cấu hình và hoạt động bình thường. - FDAS được kết nối với SPT.	Đặt FDAS ở trạng thái tĩnh lặng.	Kiểm tra chỉ báo trạng thái của SPT.	SPT phải hiển thị trạng thái theo quy định tại 5.2.1.2 và 5.2.2.6.
2.	- FATB được cấu hình và hoạt động bình thường. - FDAS được kết nối với SPT.	Kích hoạt tín hiệu báo cháy từ FDAS.	- Kiểm tra chỉ báo trạng thái SPT. - Kiểm tra tín hiệu báo cháy có được tiếp nhận tại RCT không.	- SPT phải hiển thị trạng thái theo quy định tại 5.2.1.2 và 5.2.2.6. - Tín hiệu báo cháy phải được SPT gửi tới RCT. - SPT phải hiển thị trạng thái sau khi đã nhận được tín hiệu xác nhận từ RCT theo quy định tại 5.2.1.2 và 5.2.2.6.
3.	Tiếp sau bước 2.	Đặt lại FDAS ở trạng thái tĩnh lặng.	Kiểm tra chỉ báo trạng thái của SPT.	SPT phải hiển thị trạng thái theo quy định tại 5.2.1.2 và 5.2.2.6.
4.	- FDAS được kết nối với SPT. - tạo lỗi FATB để không truyền tin giữa SPT và RCT.	Kích hoạt tín hiệu báo cháy từ FDAS.	- Kiểm tra chỉ báo trạng thái của SPT.	- SPT phải hiển thị trạng thái theo quy định tại 5.2.1.2 và 5.2.2.6.
5.	Tiếp theo sau bước 4.	Tắt và khởi động lại SPT sau đó khôi phục hoạt động bình thường của FATB.	Xem tín hiệu báo cháy được kích hoạt tại bước 4 có nhận được tại RCT không.	- Tín hiệu báo cháy được kích hoạt tại bước 4 phải được chuyển tiếp tới RCT. - SPT phải hiển thị trạng thái sau khi đã nhận được tín hiệu xác nhận từ RCT theo quy định tại 5.2.1.2 và 5.2.2.6.

6.	Lặp lại lần lượt từ bước 2 đến 5 với tín hiệu báo lỗi từ FDAS.	Lặp lại từ bước 2 đến bước 5.	Lặp lại từ bước 2 đến bước 5.	Như bước 2 đến bước 5 đối với tín hiệu báo lỗi từ FDAS.
7.	- FATB được cấu hình và hoạt động bình thường. - FDAS được kết nối với SPT.	Ngắt kết nối và khôi phục kết nối FDAS với SPT.	- Kiểm tra chỉ báo trạng thái của SPT. - Kiểm tra tín hiệu báo lỗi có được SPT tạo ra và truyền đến RCT/FAMS không.	- SPT phải hiển thị trạng thái theo quy định tại 5.2.1.2 và 5.2.2.6. - Tín hiệu báo lỗi được SPT tạo ra và truyền đến RCT/FAMS.
8.	- FATB được cấu hình và hoạt động bình thường. - FDAS được kết nối với SPT.	Ngắt và khôi phục kết nối FATP chính.	- Kiểm tra chỉ báo trạng thái của SPT. - Kiểm tra tín hiệu báo lỗi có được SPT tạo ra và truyền đến RCT/FAMS không.	- SPT phải hiển thị trạng thái theo quy định tại 5.2.1.2 và 5.2.2.6. - Tín hiệu báo lỗi được SPT tạo ra và truyền đến RCT/FAMS.
9.	- FATB được cấu hình và hoạt động bình thường. - FDAS được kết nối với SPT.	Ngắt và khôi phục kết nối FATP dự phòng.	- Kiểm tra chỉ báo trạng thái của SPT. - Kiểm tra tín hiệu báo lỗi có được SPT tạo ra và truyền đến RCT/FAMS không.	- SPT phải hiển thị trạng thái theo quy định tại 5.2.1.2 và 5.2.2.6. - Tín hiệu báo lỗi được SPT tạo ra và truyền đến RCT/FAMS.
10.	- FATB được cấu hình và hoạt động bình thường. - FDAS được kết nối với SPT.	Lỗi và khôi phục nguồn điện chính SPT.	- Kiểm tra chỉ báo trạng thái của SPT. - Kiểm tra tín hiệu báo lỗi có được SPT tạo ra và truyền đến RCT/FAMS không.	- SPT phải hiển thị trạng thái theo quy định tại 5.2.1.2 và 5.2.2.6. - Tín hiệu báo lỗi được SPT tạo ra và truyền đến RCT/FAMS.
11.	- FATB được cấu hình và hoạt động bình thường. - FDAS được kết nối với SPT.	Lỗi và khôi phục nguồn điện dự phòng.	- Kiểm tra chỉ báo trạng thái của SPT. - Kiểm tra tín hiệu báo lỗi có được SPT tạo và truyền đến RCT/FAMS.	- SPT phải hiển thị trạng thái theo quy định tại 5.2.1.2 và 5.2.2.6. - Tín hiệu báo lỗi được SPT tạo ra và truyền đến RCT/FAMS.
12.	- FATB được cấu hình và hoạt động bình thường. - FDAS được kết nối với SPT.	Kích hoạt đồng thời các tín hiệu báo lỗi và báo cháy từ FDAS.	- Kiểm tra chỉ báo trạng thái của SPT - Kiểm tra tín hiệu xác nhận được gửi từ SPT với FDAS.	- SPT phải ưu tiên hiển thị trạng thái báo cháy theo quy định tại 5.2.1.2 và 5.2.2.6. - Tín hiệu từ SPT đến RCT phải ưu tiên tín hiệu báo cháy.

E.1.2 Giao diện với FDAS

E.1.2.1 Giao diện nối tiếp chuẩn hóa với FDAS

E.1.2.1.1 Mục đích

Thử nghiệm nhằm chứng minh SPT nếu triển khai giao diện nối tiếp với FDAS, tuân thủ các yêu cầu của 5.2.1.4 và phụ lục G.

E.1.2.1.2 Nguyên tắc

Thử nghiệm bao gồm việc cấu hình SPT và FDAS theo tài liệu hướng dẫn của nhà sản xuất SPT và FDAS. Thông qua giao diện này, thực hiện truyền và tiếp nhận tin báo, cũng như khả năng xử lý lỗi tại giao diện, nối tiếp với FDAS.

Bảng E.2 - Thử nghiệm giao diện nối tiếp chuẩn hóa với FDAS

Bước	Điều kiện thử nghiệm	Quy trình thử	Phép đo	Tiêu chí đạt
1	SPT được lắp đặt và cấu hình ở trạng thái hoạt động bình thường.	Kết nối SPT với FDAS thông qua giao diện nối tiếp như theo hướng dẫn của nhà sản xuất SPT.	Kiểm tra việc kết nối SPT với FDAS có phù hợp với tài liệu hay không.	Việc kết nối SPT và FDAS phải tuân theo tài liệu hướng dẫn.
2	SPT được lắp đặt và cấu hình ở trạng thái	Tạo tín hiệu báo cháy hoặc báo lỗi trên FDAS.	Ghi lại thời gian truyền theo 5.1	Thời gian truyền phải đáp ứng quy

	hoạt động bình thường.			định tại 5.1
3	SPT được lắp đặt và cấu hình ở trạng thái hoạt động bình thường.	Ngắt kết nối giao diện nối tiếp với FDAS.	Ghi lại thời gian báo cáo lỗi (thời gian từ khi ngắt kết nối đến khi được nhận tại RCT).	Thời gian báo cáo phải theo quy định tại 5.2.1.4.1.

E.1.2.2 Giao diện song song chuẩn hóa với FDAS

E.1.2.2.1 Mục đích

Thử nghiệm nhằm chứng minh SPT nếu triển khai giao diện song song chuẩn hóa với FDAS đáp ứng quy định tại 5.2.1.4 và phụ lục G.

E.1.2.2.2 Nguyên tắc

Thử nghiệm bao gồm việc cấu hình SPT và FDAS theo tài liệu hướng dẫn của nhà sản xuất. Thông qua giao diện này, thực hiện truyền và tiếp nhận tin báo, cũng như tạo lỗi tại giao diện song song với FDAS.

Bảng E.3 - Thử nghiệm giao diện song song chuẩn hóa với FDAS

Bước	Điều kiện thử	Quy trình thử	Phép đo	Tiêu chí đạt
1	- SPT và FDAS (hoặc một trình mô phỏng giao diện FDAS tương đương) được kết nối thông qua giao diện FDAS song song và đang hoạt động theo yêu cầu. - SPT được kết nối với FATB hoạt động bình thường.	Kích hoạt một tín hiệu báo cháy từ FDAS đến tất cả các đầu vào song song của SPT theo Phụ lục G.	Ghi nhận xem có sự thay đổi điện trở cuối đường dây tại đầu vào của SPT với mức thay đổi từ 40 % trở lên so với giá trị điện trở tĩnh, duy trì trong thời gian lớn hơn 200 ms không.	Sự thay đổi điện trở cuối đường dây phải từ 40 % trở lên so với điện trở tĩnh và duy trì trong thời gian lớn hơn 200 ms. SPT nhận biết sự thay đổi là báo cháy và truyền bản tin báo cháy.
2	Như trên.	-	Đo trở kháng đầu ra báo lỗi SPT.	Trở kháng đầu ra báo lỗi SPT phải < 100 Ω khi ở trạng thái bình thường.
3	Như trên.	Gây ra lỗi FATB hoặc mô phỏng lỗi tại SPT.	Đo trở kháng đầu ra báo lỗi của SPT. Ghi nhận thời điểm chuyển trạng thái và thời gian duy trì trạng thái lỗi.	Trở kháng đầu ra báo lỗi SPT phải > 500 kΩ. Trạng thái lỗi phải được duy trì ít nhất 1 giây. Trạng thái lỗi phải được kích hoạt trong thời gian không vượt quá thời gian báo cáo lỗi.
4	Như trên.	Kích hoạt tất cả các đầu ra báo lỗi của SPT và nối từng đầu ra với một tải 20 mA.	Kiểm tra xem các đầu ra báo lỗi của SPT có đủ khả năng cho dòng điện 20 mA chạy qua khi thiết bị hoạt động hay không.	Đầu ra báo lỗi của SPT phải có khả năng chịu được dòng điện ít nhất 20 mA.
5	Như trên.	Làm thay đổi kết nối giao diện giữa FDAS và SPT bằng cách loại bỏ hoặc nối tắt đầu nối.	Ghi nhận xem có tin báo lỗi được tạo ra hay không.	Việc thay đổi kết nối giữa SPT và FDAS phải được phát hiện và báo về RCT.

E.1.2.3 Giao diện độc quyền với FDAS

E.1.2.3.1 Mục đích

Thử nghiệm nhằm chứng minh rằng giao diện độc quyền với FDAS, nếu được triển khai, đáp ứng quy định tại 5.2.1.4.

E.1.2.3.2 Nguyên tắc

Thử nghiệm được thực hiện bằng cách lắp đặt SPT theo hướng dẫn của nhà sản xuất. Sau khi lắp đặt, tiến hành kiểm tra khả năng giám sát và hiệu năng của liên kết thông qua giao diện này.

Bảng E.4 - Thử nghiệm giao diện độc quyền với FDAS

Bước	Điều kiện thử	Quy trình thử	Phép đo	Tiêu chí đạt

1	SPT được lắp đặt và cấu hình để hoạt động bình thường.	Kết nối SPT với FDAS theo tài liệu hướng dẫn.	Kiểm tra việc kết nối SPT với FDAS có phù hợp với tài liệu hướng dẫn không.	Việc kết nối SPT và FDAS phải tuân theo tài liệu hướng dẫn.
2	Như trên.	Tạo tín hiệu báo cháy hoặc báo lỗi trên FDAS.	Ghi lại thời gian truyền theo 5.1.	Thời gian truyền phải đáp ứng quy định tại 5.1.
3	Như trên.	Ngắt kết nối giao diện giữa SPT với FDAS.	Ghi lại thời gian báo cáo lỗi (thời gian từ khi ngắt kết nối đến khi RCT nhận tín hiệu lỗi).	Lỗi phải được RCT tiếp nhận. Thời gian báo cáo lỗi phải đáp ứng quy định tại 5.2.1.4.1.

E.1.3 Giám sát giao diện mạng truyền dẫn

E.1.3.1 Mục đích

Thử nghiệm nhằm chứng minh rằng SPT nếu có khả năng phát hiện và thông báo lỗi liên quan đến giao diện mạng truyền dẫn khi xảy ra sự cố mất kết nối tại từng giao diện, phù hợp với yêu cầu tại 5.2.1.5.

CHÚ THÍCH: Ví dụ về lỗi giao diện mạng bao gồm: rút cáp Ethernet, mất kết nối di động (cellular), lỗi phần cứng cổng mạng, v.v..

E.1.3.2 Nguyên tắc

Thử nghiệm được thực hiện bằng cách cố ý ngắt kết nối từng giao diện mạng của SPT khỏi mạng truyền dẫn. Sau đó, theo dõi và ghi nhận xem SPT có gửi tin báo lỗi phù hợp đến RCT hay không, trong thời gian và điều kiện quy định.

Bảng E.5 - Thử nghiệm phát hiện lỗi FATP khi giao diện mạng truyền dẫn bị lỗi

Bước	Điều kiện thử	Quy trình thử	Phép đo	Tiêu chí đạt
1	- SPT được lắp đặt và cấu hình để hoạt động bình thường. - RCT hoặc mô phỏng RCT được cung cấp để có khả năng giao tiếp với SPT.	Ngắt kết nối giao diện mạng đầu tiên (lặp lại bước 1 và 2 cho tất cả các giao diện mạng).	Theo dõi xem lỗi FATP có được ghi vào không nhật ký sự kiện không và tín hiệu lỗi có được gửi đến RCT không.	Lỗi FATP sẽ được ghi vào nhật ký sự kiện. Tín hiệu lỗi FATP sẽ được gửi đến RCT.
2	tiếp theo bước 1.	Kết nối lại giao diện mạng đã ngắt kết nối (lặp lại bước 1 và 2 cho tất cả các giao diện mạng).	- Theo dõi xem việc khôi phục lỗi FATP có được ghi nhận trong nhật ký sự kiện của SPT không. - Theo dõi xem tín hiệu khôi phục cỏ được gửi đến RCT không.	- Việc khôi phục FATP sẽ được ghi vào nhật ký sự kiện. -Tín hiệu kết nối trở lại của FATP sẽ được gửi đến RCT.

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

E.1.4 Mức độ truy cập

E.1.4.1 Mục đích

Thử nghiệm nhằm chứng minh SPT đáp ứng theo quy định tại 5.2.1.7 và Phụ lục D về việc cung cấp tối đa 4 mức độ truy cập, cũng như đảm bảo rằng việc xác thực quyền truy cập tại từng mức độ là chính xác và phù hợp với quy định.

E.1.4.2 Nguyên tắc

Thử nghiệm bao gồm việc cố gắng truy cập và sử dụng các chức năng điều khiển của SPT theo các yêu cầu được quy định tại 5.2.1.7 và Phụ lục D. Việc vận hành SPT phải được thực hiện tại từng mức truy cập cụ thể nhằm xác minh rằng các chức năng được phép truy cập tại mỗi mức có thể thực hiện thành công và các chức năng không được phép tại mức đó phải bị từ chối truy cập.

Bảng E.6 - Thử nghiệm mức độ truy cập

Bước	Điều kiện thử	Quy trình thử	Phép đo	Tiêu chí đạt
1	- SPT chưa được cấu hình. - Các thiết bị và điều kiện	Thực hiện cấu hình lần đầu cho SPT và giữ nguyên khóa mặc định.	Ghi nhận xem có hoàn tất quá trình cấu hình không.	Không được hoàn tất cấu hình nếu giữ nguyên khóa mặc định.

	cần thiết để cấu hình SPT phải có sẵn.			
2	SPT và các thiết bị cần thiết đã được lắp đặt và cấu hình để hoạt động bình thường.	Tại mức truy cập 1, cố gắng sử dụng các chức năng và điều khiển được nhà sản xuất quy định cho mức này.	Ghi lại xem có được phép truy cập hay không.	Quyền truy cập phải phù hợp với 5.2.1.7.
3	Như bước 2	Lặp lại như bước 2 cho mức truy cập 2.	Ghi lại xem có được phép truy cập hay không.	Quyền truy cập phải phù hợp với 5.2.1.7.
4	Như bước 2	Lặp lại như bước 2 cho mức truy cập 3.	Ghi nhận xem quyền truy cập mức 3 chỉ được cấp nếu người dùng mức 2 cho phép.	Quyền truy cập phải phù hợp với 5.2.1.7.
5	Như bước 2	Cố gắng truy cập bằng cách nhập sai khóa ba lần trong vòng 60 giây.	Ghi lại xem quyền truy cập có bị từ chối không.	Không được phép truy cập.
6	Tiếp theo bước 5	Chờ 80 s (± 5 s) 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 tài liệu do nhà sản xuất cung cấp chứng minh thuật toán truy cập từ xa có thể phân biệt ít nhất 1 000 000 khóa khác nhau.	Xem tài liệu.	-	Thuật toán có thể phân biệt được 1 000 000 khóa khác nhau.

E.1.5 Bảo mật chống giả mạo và bảo mật thông tin

Xác thực tài liệu nhà sản xuất SPT cung cấp phải mô tả 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 và bảo vệ thông tin được truyền bởi FATB nhằm ngăn chặn việc đọc trái phép và sửa đổi trái phép theo các yêu cầu được nêu trong 5.2.1.8.

E.1.6 Tải lên và tải xuống phần mềm và chương trình cơ sở

E.1.6.1 Mục đích

Thử nghiệm nhằm chứng minh rằng quy trình tải lên và tải xuống phần mềm hoặc chương trình cơ sở của SPT (nếu có hỗ trợ chức năng này) phù hợp với 5.2.1.10.

E.1.6.2 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 tài liệu kỹ thuật của SPT.

Bảng E.7 - Thử nghiệm tải lên và tải xuống phần mềm và chương trình cơ sở

Bước	Điều kiện thử	Quy trình thử	Phép đo	Tiêu chí đạt
1	Thiết bị SPT và các thiết bị cần thiết để cho phép SPT hoạt động theo yêu cầu phải được lắp đặt và ở trạng thái hoạt động.	Tại mức truy cập 1, thực hiện thử tải lên chương trình cơ sở.	Ghi lại xem có việc cập nhật có được cho phép hay không.	Không được phép cập nhật chương trình cơ sở.
2	Như trên	Lặp lại bước 1 tại mức truy cập 2.	Như trên	Như trên
3	Như trên	Lặp lại bước 1 tại mức truy cập 3.	Như trên	Như trên
4	Như trên	Lặp lại bước 1 tại 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. Trong quá trình cập nhật, ngắt kết nối mạng của thiết bị.	Ghi nhận liệu SPT có khôi phục hoạt động bình thường sau quá trình cập nhật không.	SPT phải hoạt động bình thường sau khi cập nhật thất bại.

E.1.7 Lưu trữ tham số

E.1.7.1 Mục đích

Thử nghiệm nhằm chứng minh khả năng của SPT trong việc duy trì dữ liệu cấu hình đặc thù của cơ sở khi mất nguồn hoặc sau chu trình khởi động lại theo quy định tại 5.2.1.11.

E.1.7.2 Nguyên tắc

Thử nghiệm bao gồm việc thay đổi ít nhất 2 tham số cấu hình đặc thù của cơ sở, sau đó tiến hành chu trình cấp lại nguồn (tắt/bật điện) và thực hiện khôi phục mặc định theo hướng dẫn sử dụng. Đọc lại các tham số đã lưu để kiểm tra tính toàn vẹn của dữ liệu sau khi mất điện và sau khi khởi động lại thiết bị.

Bảng E.8 - Kiểm tra lưu trữ tham số

Bước	Điều kiện thử	Quy trình thử	Phép đo	Tiêu chí đạt
1	SPT và các thiết bị cần thiết được lắp đặt và ở trạng thái hoạt động bình thường.	Thay đổi và lưu ít nhất 2 dữ liệu cấu hình đặc thù của cơ sở theo hướng dẫn trong tài liệu kỹ thuật.	Ghi lại xem những thay đổi có được lưu trữ hay không.	Bước này nhằm xác minh rằng dữ liệu cấu hình đã được thay đổi và lưu trữ để phục vụ các bước thử nghiệm tiếp theo.
2	Như trên	Ngắt nguồn điện SPT.	-	-
3	SPT ở trạng thái tắt nguồn.	Chờ ít nhất 10 s rồi khởi động lại SPT.	Ghi lại xem SPT có trở lại trạng thái hoạt động bình thường hay không.	SPT phải ở trạng thái hoạt động như trước khi tắt nguồn.
4	Giống như bước 1	Đọc các tham số đã thay đổi theo hướng dẫn trong tài liệu.	Ghi nhận các giá trị tham số.	Giá trị tham số phải giữ nguyên như trước khi tắt nguồn.
	Lặp lại bước 1 đến bước 4	Lặp lại bước 1 đến bước 4 theo quy trình khởi động lại trong tài liệu kỹ thuật.	Ghi nhận giá trị các tham số.	Các tham số phải giống như trước khi tắt nguồn.

E.1.8 Ghi nhật ký sự kiện

E.1.8.1 Mục đích

Thử nghiệm nhằm chứng minh rằng các sự kiện được SPT ghi lại đáp ứng yêu cầu tại Bảng 2.

E.1.8.2 Nguyên tắc

Thử nghiệm bao gồm việc tạo ra các sự kiện theo quy định trong Bảng 2, sau đó kiểm tra rằng các sự kiện này có được ghi lại trong nhật ký sự kiện của SPT không.

Bảng E.9 - Thử nghiệm ghi nhật ký sự kiện

Bước	Điều kiện thử	Quy trình thử	Phép đo	Tiêu chí đạt
1	SPT và các thiết bị cần thiết được lắp đặt và ở trạng thái hoạt động bình thường.	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 tại Bảng 2 không.	Tất cả các sự kiện đã tạo ra phải được ghi lại trong nhật ký sự kiện của SPT.

E.1.9 Bảo vệ nhật ký

E.1.9.1 Mục đích

Thử nghiệm nhằm chứng minh rằng nhật ký của SPT được bảo vệ chống lại việc xóa hoặc thay đổi nội dung dù vô tình hay cố ý theo quy định tại 5.2.1.12.

E.1.9.2 Nguyên tắc

Xác thực phương pháp mà nhà sản xuất công bố nhằm đáp ứng các yêu cầu tại 5.2.1.12 và nhật ký sự kiện được bảo vệ hiệu quả trước các hành vi xóa hoặc sửa đổi không mong muốn, bao gồm cả hành động cố ý và vô tình.

E.1.10 Dung lượng và khả năng lưu giữ nhật ký

E.1.10.1 Mục đích

Mục đích của thử nghiệm nhằm chứng minh rằng nhật ký sự kiện của SPT có thể lưu trữ tối thiểu số

lượng bản ghi sự kiện và đảm bảo thời gian lưu giữ các bản ghi đó đáp ứng theo quy định tại 5.2.1.12.

E.1.10.2 Nguyên tắc

Thử nghiệm bao gồm việc tạo các bản ghi sự kiện trong nhật ký, sau đó xác minh rằng số lượng và thời gian lưu giữ của các bản ghi này đáp ứng đầy đủ các yêu cầu được nêu tại 5.2.1.12.

Bảng E.10 - Thử nghiệm khả năng lưu trữ của nhật ký sự kiện

Bước	Điều kiện thử	Quy trình thử	Phép đo	Tiêu chí đạt
1	SPT và các thiết bị cần thiết được lắp đặt và ở trạng thái hoạt động bình thường.	Tạo 1 000 sự kiện nhật ký theo 5.2.1.12.	Kiểm tra xem tất cả các bản ghi sự kiện đã được lưu lại chưa.	Tất cả các bản ghi sự kiện phải được ghi lại đầy đủ, chính xác.
2	Như trên	Tạo số lượng sự kiện vượt quá 1 000.	Kiểm tra xem các sự kiện gần nhất có được lưu lại hay không.	Các sự kiện gần nhất phải được ghi lại đầy đủ, chính xác.
3	Như trên	Ngắt điện khỏi thiết bị trong 30 ngày sau đó cấp điện lại.	Kiểm tra xem các bản ghi sự kiện có bị ảnh hưởng hay không.	Các bản ghi sự kiện phải được lưu giữ đầy đủ, chính xác sau khi cấp lại nguồn.

E.1.11 Độ phân giải thời gian

E.1.11.1 Mục đích

Thử nghiệm nhằm chứng minh độ chính xác của dấu thời gian được gắn cho các sự kiện trong nhật ký của SPT phù hợp với yêu cầu tại 5.2.1.12.

E.1.11.2 Nguyên tắc

Thử nghiệm bao gồm việc tạo các sự kiện và kiểm tra dấu thời gian của chúng so với một nguồn thời gian tham chiếu được xác định rõ ràng. Trong thử nghiệm này, một máy chủ NTP cấp độ 2 (thường có sẵn trên Internet) có thể cung cấp độ chính xác cần thiết.

Bảng E.11 - Kiểm tra độ phân giải thời gian

Bước	Điều kiện thử	Quy trình thử	Phép đo	Tiêu chí đạt
1	SPT và các thiết bị cần thiết được lắp đặt và ở trạng thái hoạt động bình thường.	Tạo một sự kiện.	Ghi nhận dấu thời gian khi sự kiện được tạo.	Phải có bản ghi nhật ký sự kiện với độ phân giải tối thiểu 1 s và độ sai lệch so với thời gian tham chiếu không vượt quá 5 s.
2	Sau bước 1	Chờ ít nhất 72 h. Tạo thêm một sự kiện thứ hai.	Ghi nhận dấu thời gian của sự kiện (so sánh với thời gian từ nguồn tham chiếu).	Phải có bản ghi nhật ký sự kiện với độ phân giải tối thiểu 1 s và độ sai lệch so với thời gian tham chiếu không vượt quá 5 s.

E.1.12 Tài liệu

Xác thực rằng toàn bộ tài liệu bắt buộc đã được cung cấp, đầy đủ và chính xác.

E.1.13 Biện pháp xác minh hiệu năng FATB

E.1.13.1 Mục đích

Thử nghiệm nhằm chứng minh rằng các biện pháp được mô tả trong tài liệu kỹ thuật có thể được sử dụng để đo thời gian truyền, thời gian báo cáo lỗi và độ khả dụng của FATB.

E.1.13.2 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 năng của FATB hay không.

Bảng E.12 - Thử nghiệm biện pháp xác minh hiệu năng của FATB

Bước	Điều kiện thử	Quy trình thử	Phép đo	Tiêu chí đạt
1	FATB đã được lắp đặt và cấu hình để hoạt động bình thường.	Áp dụng quy trình được mô tả trong tài liệu kỹ thuật để đo thời gian truyền tin.	Kiểm tra xem quy trình có cho phép đo 3 giá trị thời gian truyền theo quy định tại 5.1.3.2 và ước tính độ chính xác của phép đo.	Quy trình phải cho phép đo và giám sát 3 giá trị thời gian truyền tin theo 5.1.3.2. Độ chính xác của phép đo không được sai lệch quá ±5 % so với mỗi giá trị thời gian tương ứng

				quy định tại 5.1.3.2.
2	Như trên	Áp dụng quy trình được mô tả trong tài liệu kỹ thuật để đo thời gian báo cáo lỗi.	Kiểm tra xem quy trình có cho phép đo 4 thời gian báo cáo lỗi theo Bảng 1 và ước tính độ chính xác của phép đo.	Quy trình phải cho phép đo và giám sát thời gian báo cáo lỗi theo quy định tại Bảng 1. Độ chính xác của phép đo không được sai lệch quá ±5 % so với mỗi giá trị thời gian tương ứng quy định tại Bảng 1.
3	Như trên	Áp dụng quy trình được mô tả trong tài liệu kỹ thuật để đo độ khả dụng của FATB và FATP.	Kiểm tra xem quy trình có cho phép đo độ khả dụng của FATB và FATP và ước tính độ chính xác của phép đo.	Quy trình phải cho phép đo và giám sát độ khả dụng. Độ chính xác của phép đo phải phù hợp với số chữ số có nghĩa tối thiểu của mức khả dụng.

E.2 Các thử nghiệm môi trường

E.2.1 Điều kiện lạnh (chế độ vận hành)

E.2.1.1 Mục đích

Chứng minh rằng SPT có thể thực hiện đúng chức năng theo yêu cầu khi hoạt động trong môi trường có nhiệt độ thấp, phù hợp với điều kiện môi trường làm việc dự kiến.

E.2.1.2 Quy trình

E.2.1.2.1 Tổng quát

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

E.2.1.2.2 Đo kiểm trước khi thử

Mẫu thử phải được thực hiện kiểm tra chức năng trước khi tác động điều kiện ổn định khi thử.

E.2.1.2.3 Trạng thái mẫu thử trong điều kiện ổn định khi thử

Lắp đặt mẫu thử theo quy định tại 7.2.1.2.2, đấu nối và cấp nguồn theo quy định tại 7.2.1.2.3. Mẫu thử phải ở trạng thái tĩnh lặng.

E.2.1.2.4 Điều kiện ổn định khi thử

Tác động điều kiện môi trường ổn định với các thông số sau:

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

- Thời gian: 16 h

E.2.1.2.5 Đo kiểm trong khi thử

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

E.2.1.2.6 Đo kiểm sau khi thử

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.

E.2.2 Điều kiện ẩm nhiệt, trạng thái ổn định (chế độ vận hành)

E.2.2.1 Mục đích

Chứng minh rằng SPT có thể thực hiện đúng chức năng trong điều kiện độ ẩm tương đối cao (không ngưng tụ), có thể xảy ra trong khoảng thời gian ngắn tại môi trường làm việc dự kiến.

E.2.2.2 Quy trình

E.2.2.2.1 Tổng quát

Thử nghiệm theo quy trình được mô tả tại TCVN 7699-2-78 (IEC 60068-2-78).

E.2.2.2.2 Đo kiểm trước khi thử

Mẫu thử phải được thực hiện kiểm tra chức năng trước khi tác động điều kiện ổn định khi thử.

E.2.2.2.3 Trạng thái của mẫu thử trong điều kiện ổn định khi thử

Lắp đặt mẫu thử theo quy định tại 7.2.1.2.2, đấu nối và cấp nguồn theo quy định tại 7.2.1.2.3. Mẫu thử

phải ở trạng thái tĩnh lặng.

E.2.2.2.4 Điều kiện ổn định khi thử

Tác động điều kiện môi trường ổn định với các thông số sau:

- Nhiệt độ: (55 ± 2) °C;

- Độ ẩm tương đối: $(93\ ^{+2}_{-3})$ %;

- Thời gian: 4 ngày.

CHÚ THÍCH: Mẫu thử phải được làm ổn định trước tại nhiệt độ (55 ± 2) °C cho đến khi đạt trạng thái ổn định về nhiệt, để tránh hiện tượng ngưng tụ nước thành giọt trên bề mặt thiết bị trong quá trình thử.

E.2.2.2.5 Đo kiểm trong khi thử

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

E.2.2.2.6 Đo kiểm sau khi thử

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.

E.2.3 Va đập (vận hành)

E.2.3.1 Mục đích

Chứng minh rằng SPT có khả năng chịu được các tác động va đập cơ học lên bề mặt trong điều kiện lắp đặt thông thường, mà không làm suy giảm chức năng hoạt động. Các tác động này được giả định là có thể xảy ra trong môi trường làm việc dự kiến của thiết bị.

E.2.3.2 Quy trình

E.2.3.2.1 Tổng quát

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

E.2.3.2.2 Đo kiểm trước khi thử

Mẫu thử phải được thực hiện kiểm tra chức năng trước khi tác động điều kiện ổn định khi thử.

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

Lắp đặt mẫu thử theo quy định tại 7.2.1.2.2, đấu nối và cấp nguồn theo quy định tại 7.2.1.2.3. Mẫu thử phải ở trạng thái tĩnh lặng.

E.2.3.2.4 Điều kiện ổn định khi thử

Tác động va đập lên tất cả các bề mặt của mẫu thử có thể tiếp cận được ở mức truy cập 1 (xem phụ lục D). Với mỗi bề mặt như vậy, tác động 3 lần lên các điểm được xem là dễ gây ra hư hại cho mẫu hoặc có thể làm hỏng sự hoạt động bình thường 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 phát hiện có hư hại ảnh hưởng đến kết quả thử, vị trí đó phải được thử lại trên một mẫu 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.

E.2.3.2.5 Đo kiểm trong 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 đảm bảo rằng kết quả của đợt 3 lần va đập không ảnh hưởng đến những đợt va đập tiếp theo.

E.2.3.2.6 Đo kiểm sau khi thử

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

E.2.4 Rung, dao động hình sin (vận hành)

E.2.4.1 Mục đích

Chứng minh rằng SPT có khả năng chịu được các tác động rung động cơ học trong điều kiện môi trường làm việc dự kiến mà không làm ảnh hưởng đến chức năng hoạt động.

E.2.4.2 Quy trình

E.2.4.2.1 Tổng quát

Thử nghiệm theo quy trình được mô tả tại TCVN 7699-2-6 (IEC 60068-2-6). Có thể kết hợp thử nghiệm trong điều kiện vận hành (mẫu thử hoạt động bình thường khi chịu rung) với thử nghiệm độ bền (mẫu thử vẫn hoạt động ổn định sau khi chịu rung kéo dài).

Thiết bị sẽ được thử rung theo từng hướng trục riêng biệt, trong một nhóm gồm 3 trục vuông góc với nhau, đảm bảo trong đó có một trục vuông góc với mặt lắp đặt mẫu thử. Mỗi trạng thái chức năng được quy định sẽ được thử nghiệm trong từng hướng rung riêng biệt.

E.2.4.2.2 Đo kiểm trước khi thử

Mẫu thử phải được thực hiện kiểm tra chức năng trước khi tác động điều kiện ổn định khi thử.

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

Lắp đặt mẫu thử theo quy định tại 7.2.1.2.2, phù hợp với TCVN 7699-2-47 (IEC 60068-2-47). đấu nối và cấp nguồn theo quy định tại 7.2.1.2.3. Tiến hành thử đối với mẫu ở trạng thái tĩnh lặng và trạng thái báo cháy.

E.2.4.2.4 Điều kiện ổn định khi thử

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 trục vuông góc nhau

- Số lượng chu kỳ theo mỗi trục: 1 cho mỗi một trạng thái chức năng

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

Theo dõi và ghi nhận mọi thay đổi hoặc sai lệch về trạng thái hoạt động của mẫu thử trong suốt khoảng thời gian chịu tác động của điều kiện ổn định khi thử.

E.2.4.2.6 Đo kiểm sau khi thử

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.

E.2.5 Tính tương thích điện từ (EMC) - thử miễn nhiễm (vận hành)

E.2.5.1 Thực hiện các phép thử tính tương thích điện từ, thử miễn nhiễm sau theo quy định trong EN 50130-4, các phép thử bao gồm:

a) Biến đổi điện áp nguồn cấp điện: Áp dụng đối với các SPT tích hợp nguồn điện bên trong hoặc có đầu vào nguồn điện phù hợp để thực hiện thử nghiệm này;

b) Sự sụt và gián đoạn điện áp nguồn cấp điện: Áp dụng đối với các SPT tích hợp nguồn điện bên trong hoặc có đầu vào nguồn điện phù hợp để thực hiện thử nghiệm này;

c) Phóng điện tĩnh điện;

d) Trường điện từ bức xạ;

e) Nhiễu dẫn gây bởi trường điện từ;

f) Đột biến nhanh;

g) Sốc chậm do điện thế năng lượng cao.

E.2.5.2 Đối với các phép thử tại E.2.5.1, phải áp dụng quy định trong IEC 62599-2 và những tiêu chí sau:

a) Thử nghiệm về chức năng trước và sau khi chịu nhiễu phải được thực hiện theo quy định tại 7.2.2 để xác minh khả năng hoạt động của mẫu thử.

b) Mẫu thử phải được lắp đặt theo hướng dẫn tại 7.2.1.2. Trạng thái vận hành của mẫu thử trong quá trình thử nghiệm phải là trạng thái tĩnh lặng.

c) Các dây kết nối đầu ra và đầu vào khác nhau phải sử dụng cáp không có vỏ bọc chống nhiễu, trừ khi nhà sản xuất yêu cầu bắt buộc phải sử dụng cáp có vỏ bọc chống nhiễu trong tài liệu kỹ thuật.

d) Trong thử nghiệm phóng tĩnh điện, các điểm tác động của máy phóng tĩnh điện phải là những điểm của mẫu thử mà có thể tiếp cận ở mức truy cập 2.

e) Trong thử nghiệm đột biến nhanh, các xung phải được truyền trực tiếp lên đường dây cấp nguồn điện xoay chiều. Các đầu khác (điều khiển, dữ liệu, tín hiệu) phải được tác động bằng phương pháp kẹp tụ (kẹp điện dung).

f) Nếu SPT có nhiều dạng đầu vào và đầu ra khác biệt, thì phải áp dụng các thử nghiệm riêng biệt

theo E. 2.5.1 mục e), f) và g) và nếu thích hợp thì cả a) và b) cho từng dạng một.

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

E.2.6.1 Mục đích

Chứng minh khả năng duy trì chức năng hoạt động của SPT ở điều kiện biến thiên điện áp nguồn cấp, trong phạm vi được nhà sản xuất quy định.

E.2.6.2 Quy trình

E.2.6.2.1 Tổng quát

Phép thử được thực hiện bằng cách cho mẫu thử hoạt động dưới từng điện áp đầu vào khác nhau theo quy định tại E.2.6.2.4 cho đến khi đạt trạng thái nhiệt độ ổn định, sau đó tiến hành kiểm tra chức năng.

E.2.6.2.2 Đo kiểm trước khi thử

Mẫu thử phải được thực hiện kiểm tra chức năng trước khi tác động điều kiện ổn định khi thử.

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

Lắp đặt mẫu thử theo quy định tại 7.2.1.2.2, đấu nối và cấp nguồn theo quy định tại 7.2.1.2.3. Mẫu thử phải ở trạng thái tĩnh lặng.

E.2.6.2.4 Điều kiện ổn định khi thử

Tác động điều kiện ổn định khi thử sau:

a) Điện áp đầu vào lớn nhất được quy định bởi nhà sản xuất;

b) Điện áp đầu vào nhỏ nhất được quy định bởi nhà sản xuất.

CHÚ THÍCH: Để đảm bảo tương thích giữa SPT và bộ nguồn sử dụng, dải điện áp đầu vào mà SPT chịu được nên bao phủ toàn bộ dải điện áp đầu ra của bộ nguồn theo TCVN 7568-4 (ISO 7240-4).

E.2.6.2.5 Đo kiểm trong quá trình thử

Tại mỗi mức điện áp đầu vào, theo dõi trạng thái của mẫu thử cho đến khi đạt nhiệt độ ổn định, sau đó tiến hành kiểm tra chức năng tương ứng.

E.2.6.2.6 Đo kiểm sau khi thử

Sau khi tác động của điều kiện ổn định khi thử, tiếp tục kiểm tra lại chức năng của mẫu thử để phát hiện bất kỳ thay đổi hoặc lỗi vận hành nào.

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

E.2.7.1 Mục đích

Chứng minh khả năng của SPT chịu được tác động lâu dài của môi trường ẩm trong điều kiện hoạt động thực tế (ví dụ như thay đổi về đặc tính điện do hấp thụ ẩm, các phản ứng hóa học trong điều kiện ẩm, ăn mòn điện hóa và các cơ chế suy giảm khác liên quan đến độ ẩm).

E.2.7.2 Quy trình

E.2.7.2.1 Tổng quát

Thử nghiệm được thực hiện theo quy trình mô tả tại TCVN 7699-2-78 (IEC 60068-2-78).

E.2.7.2.2 Đo kiểm trước khi thử

Mẫu thử phải được thực hiện kiểm tra chức năng trước khi tác động điều kiện ổn định khi thử.

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

Lắp đặt mẫu thử theo quy định tại 7.2.1.2.2, đấu nối và cấp nguồn theo quy định tại 7.2.1.2.3. Mẫu thử phải ở trạng thái tĩnh lặng.

E.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 ngày.

CHÚ THÍCH: Để tránh việc nước ngưng đọng thành giọt trên mẫu, cần đặt trước mẫu vào môi trường có điều kiện nhiệt độ ổn định ở mức (40 ± 2) °C cho đến khi đạt đến trạng thái ổn định nhiệt

E.2.7.2.5 Đo kiểm sau khi thử

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.

E.2.8 Rung, dao động hình sin (độ bền)

E.2.8.1 Mục đích

Chứng minh khả năng của SPT chịu được tác động lâu dài của hiện tượng rung ở mức độ phù hợp với môi trường lắp đặt.

E.2.8.2 Quy trình

E.2.8.2.1 Tổng quát

Sử dụng quy trình thử nghiệm mô tả tại 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.

E.2.8.2.2 Đo kiểm trước khi thử

Mẫu thử phải được thực hiện kiểm tra chức năng trước khi tác động điều kiện ổn định khi thử

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

Lắp mẫu thử theo quy định trong 7.2.1.2.2 và phù hợp với TCVN 7699-2-47 (IEC 60068-2-47) và nối với nguồn điện theo quy định tại 7.2.1.2.3. Trong quá trình chịu tác động điều kiện ổn định khi thử, không được cấp điện cho mẫu.

E.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.

E.2.8.2.5 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.

E.2.8.2.6 Đo kiểm sau khi thử

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.

E.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 F

(Quy định)

Kiểm tra, thử nghiệm bộ phận tiếp nhận tin báo cháy

F.1 Mức truy cập

F.1.1 Mục đích

Chứng minh khả năng của RCT đáp ứng quy định tại 5.3.2 và phụ lục D trong việc cung cấp 4 mức truy cập và quyền truy cập phù hợp với từng chức năng và điều khiển tương ứng.

F.1.1.1 Nguyên tắc

Thử nghiệm bao gồm việc vận hành các chức năng và điều khiển đã nêu tại 5.3.2 ở từng mức truy cập và kiểm tra xem các quyền truy cập có được cấp đúng cho các chức năng được phép và bị từ chối cho các chức năng không được phép hay không.

Bảng F.1 - Kiểm tra mức truy cập

Bước	Điều kiện thử	Quy trình thử	Phép đo	Tiêu chí đạt
1	RCT và các thiết bị cần thiết được lắp đặt và ở trạng thái hoạt động bình thường.	Tại mức truy cập 1, thử vận hành tất cả các chức năng và điều khiển được phép.	Ghi lại xem có được cấp quyền truy cập hay không.	Quyền truy cập phải phù hợp với 5.3.2.
2	Như bước 1	Lặp lại bước 1 cho mức 2.	Như trên	Như trên
3	Như trên	Lặp lại bước 1 cho mức 3.	Như trên	Như trên
4	Như trên	Lặp lại bước 1 cho mức 4.	Ghi nhận xem quyền truy cập mức 4 chỉ được cấp nếu có sự cho phép từ người dùng cấp 3.	Như trên
5	Như trên	Cố gắng truy cập bằng cách nhập sai khóa 3 lần.	Xem quyền truy cập có bị từ chối không.	Không được phép truy cập.
6	Sau bước 5	Chờ trong khoảng thời gian nhỏ hơn giá trị thời gian khóa do nhà sản xuất quy định, thử truy cập lại với khóa hợp lệ.	Ghi nhận xem có được cấp quyền truy cập hay không.	Không được phép truy cập.
7	Sau bước 5	Chờ lâu hơn thời gian quy định của nhà sản xuất, thử lại với khóa hợp lệ.	Ghi nhận xem có được cấp quyền truy cập hay không.	Được cấp quyền truy cập.
8	Như bước 1	Tiến hành cấu hình RCT mà 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 mặc định của nhà sản xuất hay không.	Phải yêu cầu thay đổi khóa mặc định, nếu không sẽ không thể hoàn tất việc cấu hình
9	Kiểm tra tài liệu của nhà sản xuất cung cấp để chứng minh thuật toán có khả năng phân biệt ít nhất 1 000 000 khóa khác nhau.	Xem xét tài liệu.	-	Tài liệu xác nhận thuật toán có thể phân biệt tối thiểu 1 000 000 khóa khác nhau.

F.2 Tải lên và tải xuống phần mềm

F.2.1 Mục đích

Chứng minh rằng rằng quá trình tải lên và tải xuống phần mềm của RCT, nếu được triển khai, đáp ứng quy định tại 5.3.3.

F.2.2 Nguyên tắc

Thử nghiệm bao gồm việc cố gắng cập nhật phần mềm của RCT, vận hành RCT ở mức truy cập phù hợp và thực hiện theo hướng dẫn trong tài liệu hướng dẫn của RCT.

Bảng F.2 - Kiểm tra tải lên và tải xuống phần mềm

Bước	Điều kiện thử	Quy trình thử	Phép đo	Tiêu chí đạt
1	RCT và các thiết bị cần thiết lắp đặt và ở trạng thái hoạt động bình thường.	Ở mức truy cập 1, cố gắng cập nhật phần mềm.	Ghi nhận việc cập nhật có được cho 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	Thực hiện cập nhật phần mềm ở mức truy cập 4. Ngắt kết nối mạng trong khi đang cập nhật phần mềm.	Ghi nhận xem RCT có ngừng hoạt động hay khôi phục bình thường không.	RCT phải tiếp tục hoạt động bình thường sau khi thử tải xuống phần mềm.

F.3 Lưu trữ tham số

F.3.1 Mục đích

Chứng minh RCT đáp ứng quy định tại 5.3.4 về khả năng chống mất dữ liệu tham số do mất nguồn điện hoặc trong quá trình khởi động lại.

F.3.2 Nguyên tắc

Tiến hành thay đổi ít nhất hai tham số liên quan đến dữ liệu cấu hình đặc thù của cơ sở, sau đó kiểm tra lại các tham số này sau một chu trình nguồn (mất điện rồi khôi phục điện) hoặc sau khi khởi động lại.

Bảng F.3 - Kiểm tra lưu trữ tham số

Bước	Điều kiện kiểm tra	Quy trình kiểm tra	Phép đo	Tiêu chí đạt
1	RCT và các thiết bị cần thiết được lắp đặt và ở trạng thái hoạt động bình thường.	Thay đổi và lưu ít nhất 2 tham số cấu hình đặc thù của cơ sở theo hướng dẫn trong tài liệu hướng dẫn	Ghi nhận xem các thay đổi có được lưu lại hay không.	-
2	Như bước 1	Tắt nguồn RCT	-	-
3	Tiếp theo bước 2 (RCT đang tắt nguồn).	Chờ ít nhất 10 s rồi bật nguồn lại.	Ghi nhận xem RCT có trở lại trạng thái hoạt động bình thường không.	RCT phải trở lại trạng thái hoạt động bình thường như trước khi tắt nguồn.
4	Như bước 1	Đọc lại các tham số đã thay đổi theo tài liệu hướng dẫn.	Ghi nhận giá trị các tham số.	Các tham số phải giữ nguyên như trước khi tắt nguồn.
5	Lặp lại bước 1 đến bước 4	Lặp lại bước 1 đến bước 4 theo quy trình khởi động lại trong tài liệu kỹ thuật.	Ghi nhận giá trị các tham số.	Các tham số phải giống như trước khi tắt nguồn.

F.4 Giám sát và thông báo lỗi FATB đến FAMS

F.4.1 Mục đích

Chứng minh RCT có khả năng phát hiện và gửi tín hiệu lỗi FATB đến FAMS đáp ứng quy định tại 5.3.5.

F.4.2 Nguyên tắc

Thử nghiệm được tiến hành bằng cách cấu hình SPT phù hợp với RCT thử nghiệm. Kết nối SPT với RCT qua hai mạng truyền dẫn khác nhau, sau đó vô hiệu SPT và ghi nhận rằng tin báo lỗi FATB được tạo ra và truyền tới FAMS trong thời gian báo cáo lỗi tối đa quy định.

F.4.3 Điều kiện

SPT ở trạng thái hoạt động bình thường, được kết nối với RCT qua hai mạng truyền dẫn sử dụng công nghệ khác nhau.

F.4.4 Quy trình

Tắt nguồn SPT để tạo ra lỗi FATB.

F.4.5 Phép đo

Ghi nhận lỗi FATB được truyền tới FAMS.

F.4.6 Tiêu chí đạt

Lỗi FATP, FATB phải được truyền tới FAMS trong thời gian báo cáo lỗi tối đa cho phép.

F.5 Giao diện với các FAMS

F.5.1 Mục đích

Chứng minh rằng giao diện giữa RCT và FAMS đáp ứng quy định tại 5.3.6.

F.5.2 Nguyên tắc

Thử nghiệm được thực hiện bằng cách tiến hành cấu hình RCT và kết nối nó với FAMS theo hướng dẫn trong tài liệu của nhà sản xuất.

Bảng F.4 - Kiểm tra giao diện với FAMS

Bước	Điều kiện thử	Quy trình thử	Phép đo	Tiêu chí đạt
1	RCT và các thiết bị cần thiết được cài đặt và ở trạng thái hoạt động bình thường.	Kết nối RCT với FAMS theo hướng dẫn tại tài liệu kỹ thuật của nhà sản xuất	Ghi nhận xem việc kết nối giữa RCT và FAMS có phù hợp với tài liệu kỹ thuật không.	Giao diện giữa RCT và FAMS phải hoạt động (thiết lập được giao tiếp).
2	Như trên	Ngắt kết nối giữa RCT và FAMS.	Ghi nhận thời gian từ khi mất kết nối cho đến khi RCT phát hiện lỗi giao tiếp với FAMS.	Thời gian thông báo lỗi phải đáp ứng quy định tại 5.3.6.

F.6 Tín hiệu lỗi

F.6.1 Mục đích

Chứng minh khả năng phát hiện và truyền tín hiệu lỗi của RCT đáp ứng quy định tại 5.3.7.

F.6.2 Nguyên tắc

Thử nghiệm bao gồm việc tạo ra các lỗi khác nhau và theo dõi xem liệu các lỗi đó có được RCT phát hiện và gửi đến FAMS không.

Bảng F.5 - Kiểm tra tín hiệu lỗi

Bước	Điều kiện thử	Quy trình thử	Phép đo	Tiêu chí đạt
1	RCT được kết nối với FAMS. FATB được cấu hình và đang hoạt động bình thường.	Tạo lỗi trong FATB.	Theo dõi xem lỗi FATB có được báo tới FAMS không.	Lỗi FATB phải được báo tới FAMS.
2	Như trên.	Tạo lỗi FATP.	Theo dõi xem lỗi FATP có được báo tới FAMS không	Lỗi FATP phải được báo tới FAMS.
3	Như trên.	Tạo lỗi giao tiếp với FAMS.	Theo dõi xem lỗi FAMS có được ghi nhận hay không.	Lỗi FAMS phải được báo theo hướng dẫn tại tài liệu kỹ thuật của nhà sản xuất.
4	Như trên.	Tạo lỗi giao diện mạng truyền dẫn.	Giám sát xem lỗi có được báo về FAMS không.	Lỗi giao diện mạng truyền dẫn phải được báo theo tài liệu kỹ thuật. Nếu lỗi này dẫn đến lỗi FATB, thì lỗi FATB phải được báo tới FAMS.

F.7 Xử lý tín hiệu

F.7.1 Mục đích

Chứng minh khả năng của RCT trong việc nhận, xử lý và chuyển tiếp tín hiệu hoặc tin báo từ FATB.

F.7.2 Nguyên tắc

Thử nghiệm bao gồm việc xác minh rằng tín hiệu hoặc tin báo được gửi đến giao diện mạng truyền dẫn của RCT có được nhận biết, xử lý chính xác và truyền tới FAMS hay không.

F.7.3 Điều kiện

RCT được lắp đặt và cấu hình theo hướng dẫn của nhà sản xuất. Thử nghiệm phải được thực hiện cho từng giao diện mạng truyền dẫn.

F.7.4 Quy trình

Tạo tín hiệu hoặc tin báo trên giao diện mạng truyền dẫn của RCT.

F.7.5 Phép đo

Ghi nhận việc RCT tiếp nhận tín hiệu hoặc tin báo.

F.7.6 Tiêu chí đạt

Tín hiệu hoặc tin báo phải được tiếp nhận, chuyển tiếp và hiển thị tại FAMS.

F.8 Ghi lại sự kiện

F.8.1 Mục đích

Chứng minh khả năng của RCT trong việc ghi nhận tất cả các sự kiện liên quan đến các chức năng đã triển khai và bảo vệ chúng khỏi bị mất do sự cố mất nguồn, đáp ứng quy định tại 5.3.8.

F.8.2 Nguyên tắc

Tiến hành kích hoạt toàn bộ các chức năng đã triển khai và tạo ra tất cả các sự kiện được yêu cầu trong Bảng 4. Sau đó, kiểm tra xem các sự kiện này có được ghi lại trong nhật ký sự kiện của RCT không và có bị ảnh hưởng bởi sự cố mất điện hay không.

Bảng F.6 - Kiểm tra ghi lại sự kiện

Bước	Điều kiện thử	Quy trình thử	Phép đo	Tiêu chí đạt
1	RCT và các thiết bị cần thiết được cài đặt và hoạt động bình thường.	Kích hoạt toàn bộ các sự kiện theo Bảng 4, mỗi sự kiện ít nhất một lần.	Kiểm tra xem từng sự kiện có được ghi lại đúng theo tài liệu kỹ thuật hay không.	Tất cả sự kiện phải được ghi nhận đầy đủ với ngày và giờ chính xác.
2	Như trên	Tắt và khôi phục lại nguồn điện cho RCT.	Kiểm tra xem sự kiện có bị mất hoặc sai lệch không.	Tất cả sự kiện phải còn lưu giữ nguyên vẹn trong bộ ghi nhật ký.

F.9 Độ phân giải và đồng bộ hóa thời gian

F.9.1 Mục đích

Chứng minh rằng các dấu thời gian được gán cho các sự kiện trong nhật ký sự kiện của RCT đáp ứng quy định tại 5.3.8

F.9.2 Nguyên tắc

Thử nghiệm bao gồm việc tạo các sự kiện và kiểm tra dấu thời gian của chúng so với một nguồn thời gian tham chiếu được xác định rõ ràng. Trong thử nghiệm này, một máy chủ NTP cấp độ 2 (thường có sẵn trên Internet) có thể được sử dụng để cung cấp độ chính xác cần thiết.

Bảng F.7 - Kiểm tra độ phân giải và đồng bộ hóa thời gian

Bước	Điều kiện thử	Quy trình thử	Phép đo	Tiêu chí đạt
1	RCT và các thiết bị cần thiết được cài đặt và hoạt động bình thường.	Đồng bộ thời gian theo thông số kỹ thuật của nhà sản xuất.	Ghi nhận xem thời gian có được đồng bộ với giờ UTC hay không.	Thời gian phải được đồng bộ với giờ UTC.
2	RCT và các thiết bị cần thiết được cài đặt và hoạt động bình thường.	Tạo sự kiện.	Ghi lại dấu thời gian khi tạo sự kiện.	Nhật ký phải ghi lại sự kiện với độ phân giải tối thiểu 1 s và sai số so với thời gian tham chiếu nhỏ hơn 5 s.
3	Sau bước 2	Chờ ít nhất 72h và tạo sự kiện thứ hai.	Ghi nhận dấu thời gian của sự kiện thứ hai và so sánh với thời gian tham chiếu.	Nhật ký phải ghi lại sự kiện với độ phân giải tối thiểu 1 s và sai số so với thời gian tham chiếu nhỏ hơn 5 s.

F.10 Độ bền của nhật ký

Xác thực rằng tài liệu kỹ thuật của nhà sản xuất nêu rõ cách thức đảm bảo dữ liệu nhật ký sự kiện được lưu giữ bền vững trong 3 năm.

F.11 Tối ưu hóa phương pháp lưu trữ sự kiện

F.11.1 Mục đích

Chứng minh rằng nếu RCT áp dụng phương pháp tối ưu hóa lưu trữ sự kiện bằng cách nhóm các sự kiện giống nhau, thì việc ghi nhận phải đáp ứng quy định tại 5.3.8.

F.11.2 Nguyên tắc

Thử nghiệm bao gồm việc tạo ra các chuỗi sự kiện giống hệt nhau, xảy ra liên tiếp, sau đó kiểm tra xem chúng có được ghi lại trong RCT phù hợp với yêu cầu tại mục 5.3.8 hay không.

Bảng F.8 - Kiểm tra tối ưu hóa nhật ký

Bước	Điều kiện kiểm tra	Quy trình kiểm tra	Phép đo	Tiêu chí đạt
1	RCT và các thiết bị cần thiết được cài đặt	Tạo ra một chuỗi các sự kiện giống hệt	Kiểm tra xem các sự kiện được ghi	Tất cả các sự kiện phải được ghi với dấu thời gian

	và hoạt động bình thường.	nhau, xảy ra liên tiếp.	nhận có tuân thủ quy định tại 5.3.8 hay không.	chính xác, và số lượng sự kiện giống nhau phải được ghi nhận đúng.

F.12 Nhận dạng người dùng cho các mục nhật ký

F.12.1 Mục đích

Chứng minh rằng mọi hành động do người dùng (bao gồm thay đổi cấu hình, thêm/xóa/sửa người dùng hoặc quyền truy cập, thay đổi thủ công ngày và giờ, cập nhật phần mềm, truy cập vào RCT) đều được ghi nhận trong nhật ký sự kiện kèm theo thông tin nhận dạng người dùng đã thực hiện hành động đó.

F.12.2 Nguyên tắc

Thử nghiệm bao gồm việc tạo ra sự kiện nhật ký nêu tại F.12.1, sau đó kiểm tra rằng tất cả các sự kiện này có được ghi nhận đúng cách theo yêu cầu hay không.

Bảng F.9 - Kiểm tra nhận dạng người dùng trong nhật ký

Bước	Điều kiện thử	Quy trình thử	Phép đo	Tiêu chí đạt
1	RCT và các thiết bị cần thiết được lắp đặt và hoạt động bình thường.	Tạo ít nhất một sự kiện nhật ký thuộc các loại liệt kê tại F.12.1	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 thông tin nhận dạng người dùng.

F.13 Chế độ vận hành

F.13.1 Mục đích

Chứng minh rằng tất cả các chế độ vận hành được hỗ trợ đều đáp ứng quy định tại 5.3.9. Tài liệu của nhà sản xuất phải nêu rõ các chế độ vận hành mà RCT được hỗ trợ

F.13.2 Nguyên tắc

Thử nghiệm bao gồm việc kích hoạt tín hiệu báo cháy hoặc báo lỗi từ FDAS hoặc SPT tới RCT, theo dõi xem RCT có chuyển tín hiệu xác nhận tới SPT trong các điều kiện giao tiếp khác nhau giữa RCT và FAMS hay không.

Bảng F.10 - Kiểm tra chế độ vận hành

Bước	Điều kiện thử	Quy trình thử	Phép đo	Tiêu chí đạt
1	RCT được kết nối với FAMS và FATB đang hoạt động bình thường.	Kích hoạt tin báo cháy từ FDAS hoặc tin báo lỗi từ SPT tới RCT.	Theo dõi xem tin báo có được hiển thị tại FAMS trong thời gian quy định hay không.	tin báo phải hiển thị tại FAMS.
2	Ngắt kết nối RCT với FAMS, bảo đảm không thể truyền tin báo giữa RCT và FAMS.	Kích hoạt tin báo cháy từ FDAS hoặc tin báo lỗi từ SPT tới RCT.	Theo dõi xem tin báo có hiển thị tại FAMS không.	Không có tin báo hiển thị tại FAMS.
3	Tiếp theo bước 2, chờ ít nhất 30 giây.	Kết nối lại RCT và FAMS.	Theo dõi xem tin báo đã kích hoạt trong bước 2 có được hiển thị tại FAMS không.	tin báo phải hiển thị tại FAMS.

F.14 Tấn công từ chối dịch vụ

F.14.1 Mục đích

Xác minh tài liệu kỹ thuật của nhà sản xuất để chứng minh rằng việc tấn công DoS vụ trên một giao diện mạng truyền dẫn không làm ảnh hưởng bất lợi đến hoạt động của RCT hoặc bất kỳ giao diện mạng truyền dẫn nào khác.

F.14.2 Nguyên tắc

Thử nghiệm được thực hiện thông qua việc kiểm tra tài liệu kỹ thuật của nhà sản xuất nhằm xác minh rằng RCT đã được thiết kế hoặc có cơ chế bảo vệ phù hợp để hạn chế tác động của tấn công DoS.

F.14.3 Quy trình kiểm tra

Kiểm tra tài liệu kỹ thuật của nhà sản xuất liên quan đến RCT.

F.14.4 Phép đo

Kiểm tra xem trong tài liệu có mục liên quan đến tấn công DoS, trong đó nêu rõ rằng việc tấn công DoS vào một giao diện mạng truyền dẫn không gây ảnh hưởng bất lợi đến hoạt động của RCT hoặc

đến hoạt động của bất kỳ giao diện mạng truyền dẫn nào khác của RCT.

F.14.5 Tiêu chí đạt

Tài liệu của nhà sản xuất phải tồn tại nội dung mô tả RCT đã có thiết kế hoặc cơ chế bảo vệ phù hợp để hạn chế tác động của tấn công DoS.

F.15 Bảo mật thông tin và bảo mật chống giả mạo

F.15.1 Nhà sản xuất phải mô tả trong tài liệu kỹ thuật của RCT các phương pháp được sử dụng nhằm bảo vệ chống lại việc thay thế SPT bằng thiết bị giả lập hoặc thiết bị tương tự, phù hợp với quy định tại 5.3.12.

F.15.2 Nhà sản xuất phải mô tả trong tài liệu kỹ thuật của RCT các phương pháp để bảo vệ thông tin được truyền qua FATB nhằm ngăn chặn hành vi đọc trái phép hoặc chỉnh sửa trái phép, phù hợp với quy định tại 5.3.11.

F.16 Dự phòng RCT

F.16.1 Mục đích

Chứng minh rằng hệ thống vẫn duy trì khả năng truyền và tiếp nhận tin báo tại FAMS khi một trong các RCT bị vô hiệu hóa hoặc mất kết nối mạng. Trong trường hợp tất cả các giao diện mạng truyền dẫn của cả hai RCT bị mất kết nối, hệ thống phải phát hiện và báo lỗi FATB đến FAMS.

F.16.2 Nguyên tắc

Tạo tin báo cháy hoặc báo lỗi từ SPT đến RCT trong các điều kiện: bình thường (khi tất cả các RCT đều hoạt động); điều kiện lỗi (khi một trong hai RCT bị vô hiệu hóa) và khi tất cả giao diện mạng truyền dẫn của cả hai RCT bị lỗi. Kiểm tra tại FAMS các tin báo có được tiếp nhận đúng theo yêu cầu hay không.

Bảng F.11 - Kiểm tra dự phòng RCT

Bước	Điều kiện thử	Quy trình thử	Phép đo	Tiêu chí đạt
1	FATB hoạt động bình thường, cả hai RCT đều được kết nối với FAMS.	Kích hoạt tin báo cháy hoặc tin báo lỗi từ SPT tới RCT.	Kiểm tra xem tin báo có được nhận tại FAMS không.	Tin báo phải được tiếp nhận tại FAMS.
2a	FATB vẫn đang hoạt động bình thường. Vô hiệu hóa một RCT (RCT1), RCT còn lại (RCT2) vẫn đang hoạt động.	Kích hoạt tin báo cháy hoặc tin báo lỗi từ SPT tới RCT.	Kiểm tra xem tin báo có được nhận tại FAMS không.	Tin báo phải được nhận tại FAMS.
2b	FATB vẫn đang hoạt động bình thường. Vô hiệu hóa RCT2, RCT1 vẫn đang hoạt động.	Kích hoạt tin báo cháy hoặc tin báo lỗi từ SPT tới RCT.	Kiểm tra xem tin báo có được nhận tại FAMS không.	Tin báo phải được nhận tại FAMS.
3	FATB vẫn đang hoạt động bình thường. Vô hiệu hóa toàn bộ các giao diện mạng truyền dẫn của cả RCT1 và RCT2.	Kích hoạt tin báo cháy hoặc tin báo lỗi từ SPT tới RCT.	Kiểm tra tại FAMS xem có tin báo lỗi FATB hay không.	Lỗi FATB phải được nhận tại FAMS.

F.17 Tài liệu

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

Phụ lục G

(Quy định)

Giao diện giữa hệ thống báo cháy và thiết bị truyền tin báo cháy

G.1 Giao diện song song giữa FDAS và SPT

G.1.1 Tổng quan

Khi giao diện song song được cung cấp, giao diện này phải hoạt động như mô tả tại G.1.2 và G.1.3 phụ lục này. Tối thiểu, giao diện song song phải cung cấp hai đầu vào (gồm một đầu vào báo cháy và một đầu vào báo lỗi của FDAS) và một đầu ra báo lỗi.

G.1.2 Đầu vào báo cháy và báo lỗi

Việc giám sát các đầu vào của SPT phải được thực hiện bởi chính SPT. Nếu điện trở cuối đường dây thay đổi 40 % trở lên và sự thay đổi này kéo dài hơn 200 ms, thì trạng thái đầu vào phải được coi là đã thay đổi.

G.1.3 Đầu ra báo lỗi

G.1.3.1 Tổng quan

Tất cả các đầu ra báo lỗi phải là tiếp điểm không mang điện áp hoặc kiểu cực thu hở. Nếu đầu ra là cực thu hở, đầu ra phải có khả năng tiêu thụ dòng tối thiểu 20 mA.

G.1.3.2 Lỗi FATB

Đầu ra báo lỗi phải tuân thủ các yêu cầu sau:

a) Ở trạng thái bình thường (không có lỗi): đầu ra đóng (điện trở < 100 Ω);

b) Trong trường hợp lỗi FATB: đầu ra mở (điện trở > 500 kΩ);

c) Trong trường hợp lỗi SPT: đầu ra mở (điện trở > 500 kΩ);

d) Thời gian kích hoạt đầu ra lỗi phải tương ứng với thời gian tồn tại của lỗi, nhưng không được dưới 1 s.

G.2 Giao diện nối tiếp giữa FDAS và SPT

G.2.1 Có thể kết nối FDAS và SPT bằng bất kỳ giao diện nối tiếp và phương tiện truyền tín hiệu nào. Trong trường hợp kết nối giữa FDAS và SPT sử dụng thiết bị hoặc hệ thống trung gian có tính năng chủ động như bộ chuyển đổi tín hiệu, bộ định tuyến hoặc bất kỳ thiết bị hoặc hệ thống tương tự nào khác thì các thiết bị hoặc hệ thống này phải được coi là một phần của FDAS hoặc SPT và do đó phải đảm bảo các quy định có liên quan của FDAS và SPT.

G.2.2 Nhà sản xuất phải chỉ định giao diện nối tiếp giữa SPT và FDAS theo Mô hình tham chiếu OSI, lớp 7 (lớp ứng dụng).

G.2.3 Mô tả kỹ thuật giao diện phải bao gồm ít nhất các lớp vật lý, liên kết dữ liệu và lớp ứng dụng.

G.2.4 Giao thức nối tiếp sẽ cho phép phát hiện bất kỳ sự cố nào của kết nối trong thời gian báo cáo lỗi quy định tại tiêu chuẩn này.

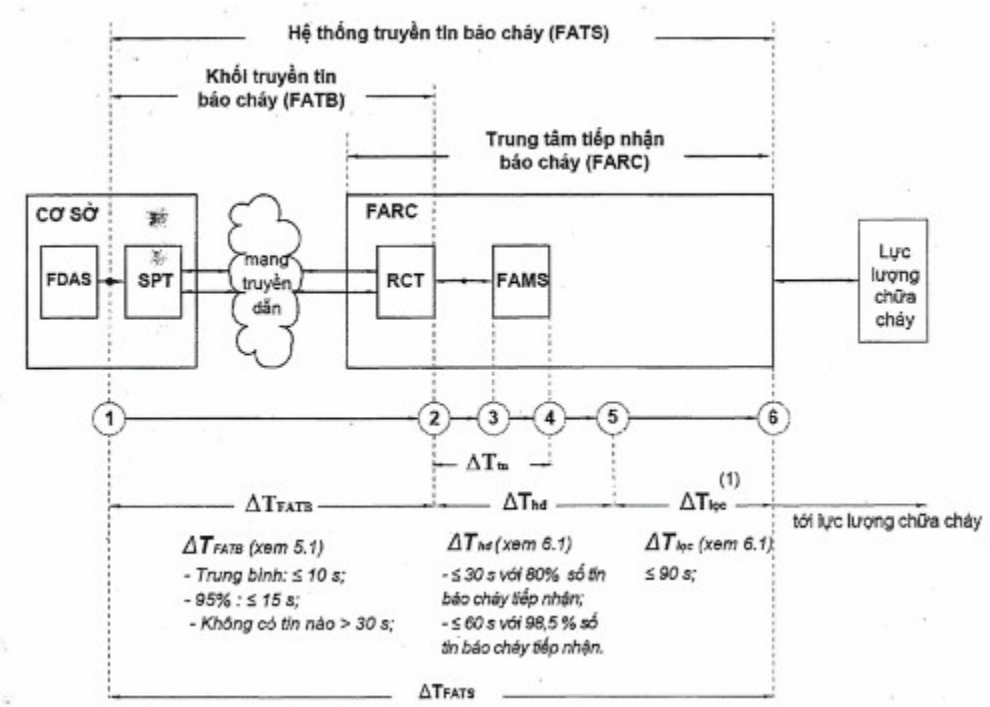
G.2.5 Nhà sản xuất sẽ cung cấp kết quả thử nghiệm và tài liệu nêu rõ khả năng tương thích với FDAS và FATB.

Phụ lục H

(Tham khảo)

Xử lý tin báo cháy hệ thống truyền tin báo cháy

H.1. Các mốc thời gian xử lý tin báo cháy



Hình H.1 - Mốc thời gian xử lý tin báo trong FATS.

CHÚ DẪN:

(1): Có thể có hoặc không.

① **- T_{SPT}**: Thời điểm tin báo (báo cháy hoặc báo lỗi) được trình bày tại giao diện giữa FDAS và SPT;

② **- T_{RCT}**: Thời điểm RCT bắt đầu gửi tin báo đến FAMS;

③ - **T_{FAMS}**: Thời điểm FAMS nhận tin báo;

④ **- T_{tn}**: Thời điểm nhân viên FARC nhận thông tin hoặc thời điểm FARC kích hoạt một cảnh báo tự động;

⑤ **- $T_{hđ}$**: Thời điểm hành động đầu tiên được thực hiện bởi nhân viên FARC hoặc FAMS theo quy trình đã định;

⑥: Thời điểm kết thúc việc lọc tin báo cháy;

ΔT_{FATB}: Thời gian truyền trong FATB (xem 5.1);

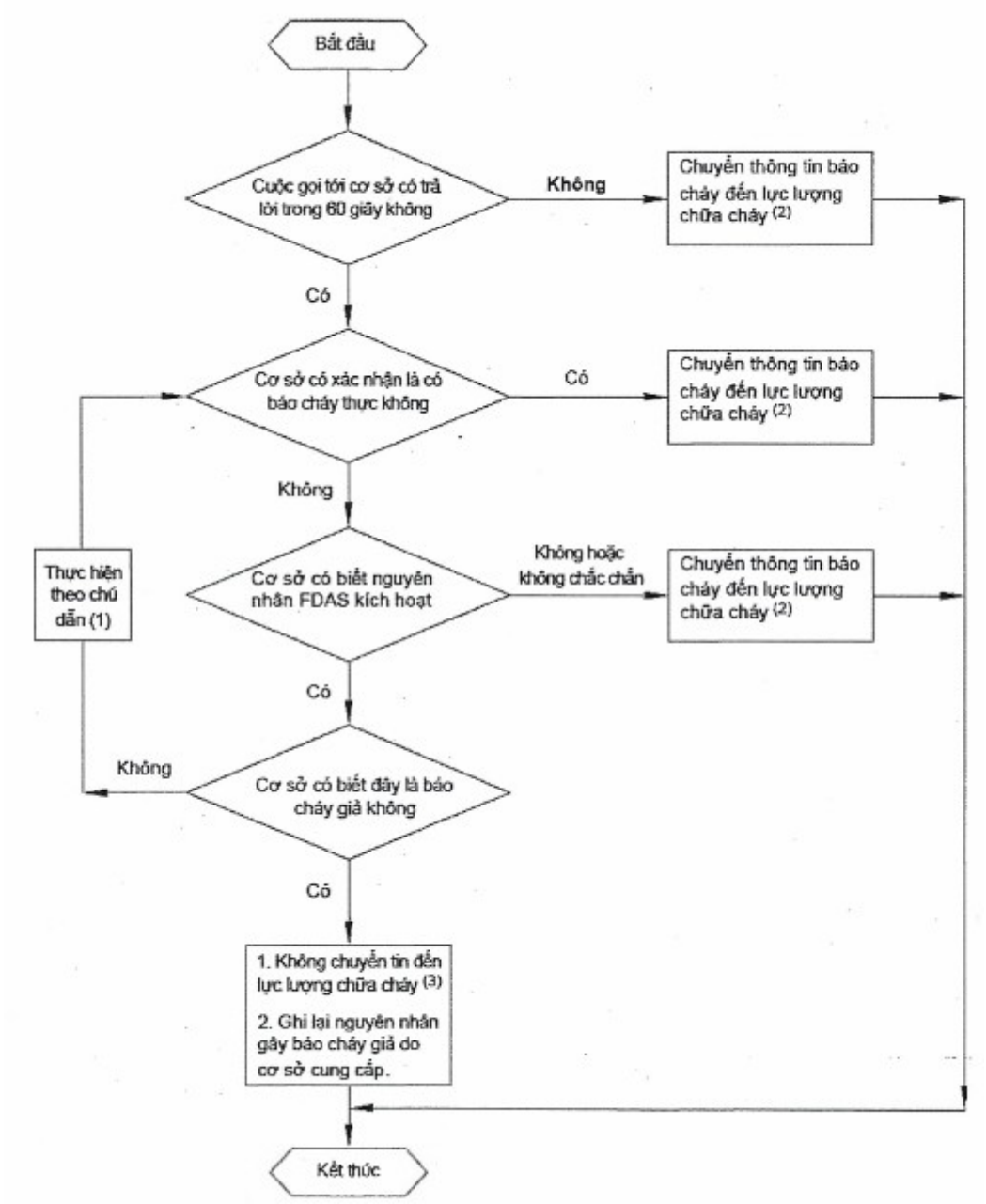
ΔT_{tn}: Khoảng thời gian từ khi RCT bắt đầu gửi tin báo đến thời điểm nhân viên FARC nhận biết hoặc thời điểm FARC kích hoạt một hành động tự động ($\Delta T_{tn} = T_{tn} - T_{RCT}$);

$\Delta T_{hđ}$: Khoảng thời gian từ khi RCT gửi tin báo đến thời điểm hành động đầu tiên được thực hiện bởi nhân viên FARC hoặc FAMS theo quy trình đã định ($\Delta T_{hđ} = T_{hđ} - T_{RCT}$);

$\Delta T_{lọc}$: Thời gian lọc tin báo cháy (xem 6.1)

ΔT_{FATS}: Thời gian từ khi tin báo cháy có sẵn tại đầu ra của FDAS cho tới thời điểm tin báo cháy bắt đầu được chuyển từ FARC tới lực lượng chữa cháy.

H.2. Sơ đồ logic quá trình lọc tin báo cháy



Hình H.2 - Sơ đồ logic quá trình lọc tin báo cháy

CHÚ DẪN:

(1): Không được lặp đi lặp lại việc hỏi lại cơ sở nhiều hơn một lần. Trong trường hợp người tại cơ sở không thể đưa ra phản hồi chính xác (người tại cơ sở không biết mình cần phải xác nhận gì, không rõ đang có cháy thật hay không, hoặc không có quyền quyết định thông tin thì xem như không thể xác minh), thì điều này phải được xác định từ trước trong quá trình đánh giá rủi ro và hệ thống phải có sẵn biện pháp lọc thay thế phù hợp (ví dụ, gọi cho một người khác có quyền xác minh...). Nếu không thể xác nhận chắc chắn là báo cháy giả, thì tín hiệu báo cháy phải được xử lý như báo cháy thực và chuyển tới lực lượng chữa cháy.

(2): Thông báo cho lực lượng chữa cháy phải ghi rõ kết quả lọc báo cháy (Ví dụ: Tin báo cháy đã được xác nhận; không liên hệ được với cơ sở; cơ sở không xác định hoặc không chắc chắn có báo cháy thật hay không...)

(3): Khi tin báo cháy không được gửi đến lực lượng chữa cháy, phải thông báo rõ ràng cho cơ sở rằng nếu sau đó phát hiện thấy cháy thật hoặc nghi ngờ có cháy thì cần khởi tạo một thông báo cháy mới (qua FATP bằng cách nhấn nút báo cháy, gọi đến Trung tâm tiếp nhận báo cháy hoặc các hình thức khác) để thông tin kịp thời gửi tới lực lượng chữa cháy.

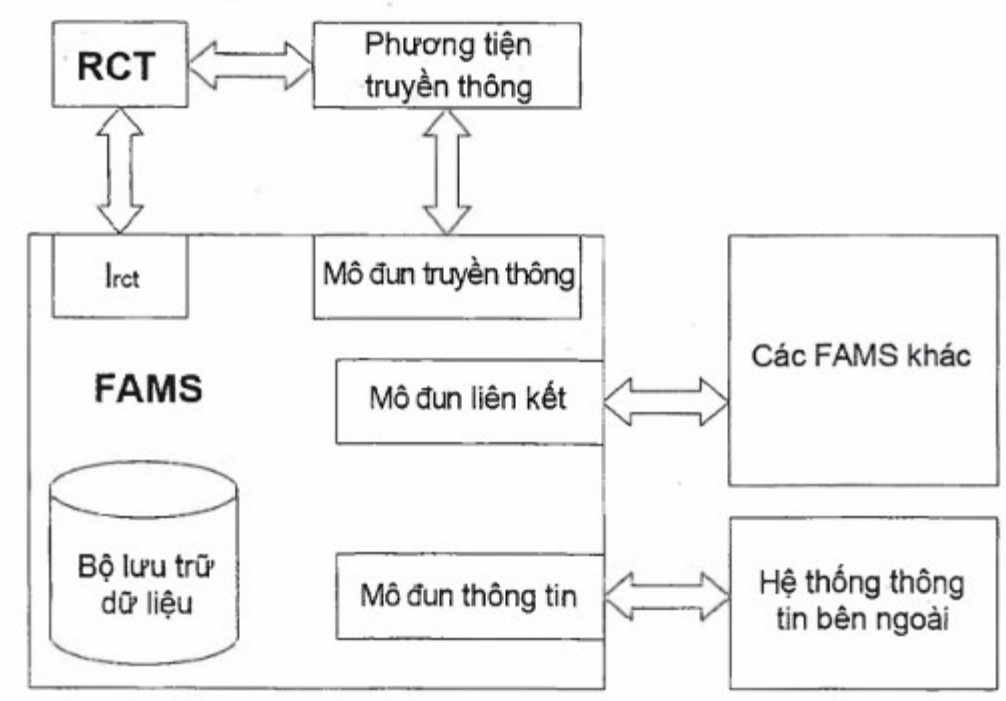
Phụ lục I

(Tham khảo)

Hệ thống quản lý tin báo cháy

I.1 Cấu trúc của FAMS

I.1.1 FAMS là một phần mềm chạy trên một hoặc nhiều máy tính có bộ lưu trữ dữ liệu vật lý đi kèm. Hệ thống có thể bao gồm một hoặc nhiều mô-đun phần mềm (ví dụ: Mô-đun giao tiếp với RCT; Mô-đun truyền thông; Mô-đun thông tin; Mô-đun kết nối, v.v.).



Hình I.1 - Hệ thống quản lý tin báo cháy

I.1.2 Giao diện kết nối với RCT (I_{RCT})

I.1.2.1 FAMS có thể được tích hợp cùng RCT hoặc có thể là một thiết bị hoặc hệ thống độc lập miễn là đáp ứng được các yêu cầu của tiêu chuẩn này.

I.1.2.2 Nhiều RCT của các nhà sản xuất khác nhau có thể được kết nối với một FAMS thông qua một mô-đun giao diện (I_{RCT}).

I.1.3 Kết nối với các FAMS khác (mô-đun liên kết)

I.1.3.1 Các FAMS khác nhau (trong cùng một FARC hoặc ở nhiều FARC khác nhau) có thể kết nối với nhau thông qua các mô-đun liên kết.

I.1.3.2 Đường truyền dữ liệu giữa hai hoặc nhiều FAMS bảo đảm yêu cầu về bảo mật và hiệu năng tối thiểu như đối với yêu cầu của FATB tại tiêu chuẩn này.

I.1.4 Mô-đun truyền thông

I.1.4.1 Mô-đun truyền thông được sử dụng để kết nối với các thiết bị truyền thông bên ngoài (ví dụ: email, fax, máy in, điện thoại, v.v.).

I.1.4.2 Khả năng tương thích giữa mô-đun truyền thông và các thiết bị liên lạc bên ngoài phải được lập thành tài liệu và được kiểm tra đầy đủ.

I.1.5 Mô-đun thông tin

Mô-đun này được sử dụng để kết nối với các hệ thống thông tin bên ngoài, cung cấp dữ liệu hỗ trợ quá trình xử lý thông tin báo cháy, ví dụ: thông tin giao thông, thông tin thời tiết, hạ tầng dữ liệu liên quan đến khu vực xảy ra cháy.

I.1.6 Giao diện người dùng

Giao diện dành cho nhân viên vận hành tại FARC phải là một phần của FAMS. Ngoài ra, cũng có thể kết nối FAMS với một FAMS khác thông qua mô-đun liên kết, và tại đó có thể cung cấp giao diện người dùng phục vụ người vận hành FARC từ xa.

I.2 Giám sát lỗi

I.2.1 Tổng quan

FAMS phải giám sát các chức năng của chính nó hoạt động, cũng như chức năng của các thành phần phần cứng và phần mềm liên quan (ví dụ: bộ giám sát phần mềm - software watchdog).

I.2.2 Phát hiện lỗi

FAMS phải có khả năng phát hiện các lỗi sau đây:

- Sự cố hoặc lỗi một phần trong FAMS;

- Nhập dữ liệu thủ công chứa dữ liệu không hợp lệ;

- Nhận dữ liệu mà FAMS không thể giải mã hoặc xử lý đúng cách;

I.2.3 Tránh lỗi khi nhập dữ liệu thủ công

Việc nhập dữ liệu không chính xác hoặc không hợp lệ phải được ngăn chặn bằng cách kiểm tra tính hợp lệ của nội dung nhập. Quy định này được áp dụng đối với những trường nhập liệu mà việc kiểm tra như vậy là hợp lý và khả thi về mặt logic.

I.2.4 Hiển thị thông tin lỗi

Thông tin về lỗi phải được hiển thị trong vòng 10 s kể từ khi lỗi xảy ra, trừ khi có quy định khác.

I.3 Xử lý tin báo

I.3.1 Xác nhận tin báo

I.3.1.1 Tin báo chỉ được FAMS xác nhận sau khi đã được lưu trữ an toàn (ví dụ: trong hàng đợi tin báo được bảo vệ hoặc trong nhật ký).

I.3.1.2 Các mốc hoặc khoảng thời gian có liên quan đến quá trình xác nhận tin báo phải được nhà sản xuất FAMS nêu rõ trong tài liệu kỹ thuật.

I.3.2 Tin báo cháy

I.3.2.1 Khi không có tin báo cháy nào khác đang được xử lý, tin báo cháy mới phải được hiển thị trong vòng 5 s sau khi xác nhận, để chờ nhân viên vận hành chấp nhận tin báo.

I.3.2.2 Một tín hiệu cảnh báo (ví dụ: âm thanh và/hoặc hình ảnh) phải được tạo ra đồng thời với việc hiển thị tin nhắn, để thông báo cho nhân viên vận hành FARC.

CHÚ THÍCH: Nếu hệ thống đang phát tín hiệu cảnh báo, thì khi có một tin báo cháy mới xuất hiện và được xác nhận, tín hiệu cảnh báo đó có thể được khởi động lại từ đầu.

I.3.3 Tin báo lỗi

Tin báo lỗi từ FDAS cũng như các tin báo lỗi khác phải được xử lý theo cách tương tự xử lý tin báo cháy (I.3.2 Phụ lục I).

I.3.4 Thông báo dự kiến

I.3.4.1 Các thông báo dự kiến, nếu được FAMS nhận đúng trong khoảng thời gian đã được lên kế hoạch trước, thì không cần phải hiển thị, với điều kiện là sau khi đã được xác nhận, việc xử lý được FAMS thực hiện tự động.

I.3.4.2 Nếu FAMS không nhận được các thông báo dự kiến và không xác nhận trong thời gian đã định, thì FAMS phải tạo một thông báo và xử lý thông báo đó như một tin báo cháy (I.3.2 Phụ lục I)

I.3.4.3 FAMS phải có khả năng hiển thị các thông báo dự kiến khi có yêu cầu.

CHÚ THÍCH 1: Thông báo dự kiến không phải các tin báo cháy hoặc báo lỗi nhưng phải được FARC nhận được theo lịch trình định trước. Các thông báo dự kiến thường là thông báo trạng thái, được gửi từ FATB, FARC đến FAMS nhằm mục đích giám sát tình trạng hoạt động của thiết bị, hệ thống.

CHÚ THÍCH 2: Khoảng thời gian đã được lên kế hoạch trước là khoảng thời gian cụ thể đã được cấu hình từ trước trong FAMS, nhằm quy định khi nào một thông báo dự kiến phải được gửi và nhận. Khoảng thời gian này có thể định kỳ theo chu kỳ (ví dụ 10s, 20s) hoặc theo lịch cố định (19h00 hàng ngày) nhằm giám sát tính liên tục, độ tin cậy của hệ thống. Khi không nhận được các thông báo này theo lịch, hệ thống được coi là lỗi và xử lý theo quy trình báo lỗi.

I.3.5 Các thông báo khác nhận được

Nếu FAMS có khả năng tiếp nhận các thông báo khác ngoài những thông báo được mô tả trong I.3.2, I.3.3 và I.3.4 Phụ lục I, thì hệ thống phải có khả năng xử lý và hiển thị các thông báo này theo yêu cầu đã định trước.

I.3.6 Hàng đợi tin báo

I.3.6.1 FAMS phải có cơ chế hàng đợi tin báo.

I.3.6.2 Các tin báo đến phải được truy xuất từ hàng đợi theo thứ tự thời gian đến, trừ khi FAMS cỏ chức năng ưu tiên mức độ đầu vào. Trong trường hợp có chức năng ưu tiên, các tin báo phải được truy xuất theo quy định tại I.3.7 Phụ lục I.

I.3.6.3 FAMS phải cung cấp một chỉ báo khi có một hoặc nhiều tin báo đang nằm trong hàng đợi. Trường hợp có nhiều tin báo, FAMS phải chỉ báo sự tồn tại của các tin báo trong vòng 5s kể từ khi các tin báo đó được xác nhận; chỉ báo này không được làm gián đoạn việc hiển thị các tin báo đang được xử lý hoặc đang chờ được chấp nhận trong hàng đợi.

I.3.6.4 Sau mỗi lần nhân viên vận hành chấp nhận một bản tin, FAMS phải cập nhật trạng thái hàng đợi (giảm số lượng, hiển thị bản tin kế tiếp...) trong vòng 5 giây.

I.3.6.5 Khi có yêu cầu, FAMS phải có chức năng hiển thị các tin báo đến từ một FDAS duy nhất. Tin báo từ một FDAS duy nhất phải được hiển thị theo thứ tự thời gian nhận được.

I.3.6.6 Dung lượng của hàng đợi tin báo phải được quy định trong tài liệu của nhà sản xuất FAMS. Một tín hiệu cảnh báo phải được kích hoạt khi hàng đợi tin báo đạt 90 % dung lượng. Nếu hàng đợi tin báo đã đầy, FAMS không được xác nhận các tin báo mới đến.

I.3.7 Ưu tiên đầu vào

I.3.7.1 Nếu FAMS có chức năng ưu tiên mức độ đầu vào, các tin báo phải được truy xuất khỏi hàng đợi theo các mức độ ưu tiên.

I.3.7.2 Phương pháp xác định mức độ ưu tiên đầu vào phải được nhà sản xuất FAMS quy định trong tài liệu (ví dụ: loại tin báo; thứ tự xử lý các loại tin báo ưu tiên..., v.v.).

I.3.7.3 Trường hợp có nhiều tin báo có cùng mức độ ưu tiên trong hàng đợi, chúng phải được truy xuất theo thứ tự thời gian nhận được.

I.3.8 Chỉ báo cảnh báo

I.3.8.1 FAMS phải cung cấp chỉ báo cảnh báo khi tin báo được hiển thị. Chỉ báo cảnh báo phải được kích hoạt trong vòng 5 s sau khi một tin báo được FAMS xác nhận hoặc khi có thông tin nội bộ được tạo ra trong hệ thống. Chỉ báo cảnh báo nên dừng khi tin báo được nhân viên vận hành chấp nhận.

I.3.8.2 FAMS cũng phải có phương pháp để dừng chỉ báo cảnh báo phát sinh từ việc chỉ báo cảnh báo kích hoạt do xác nhận các tin báo không phải là tin báo cháy hoặc từ việc tạo ra thông tin cục bộ (bên trong FARC). Tính năng này chỉ dành cho người dùng có quyền truy cập mức 2.

I.3.8.3 FAMS có thể có chức năng cho phép bật hoặc tắt tính năng kích hoạt chỉ báo cảnh báo khi có tin báo đến. Tuy nhiên, chức năng này phải bị tự động vô hiệu hóa khi hàng đợi không có tin báo cháy. Quyền truy cập vào tính năng này chỉ được sử dụng bởi người có quyền truy cập mức 3.

I.3.9 Chấp nhận tin báo

I.3.9.1 Phải có một cơ chế cho phép chấp nhận tin báo. Khi tin báo đang hiển thị được chấp nhận, phải dừng chỉ báo cảnh báo và loại bỏ tin báo đó khỏi hàng đợi để cho phép hiển thị tin báo tiếp theo trong hàng đợi (nếu có).

I.3.9.2 Phải có phương thức đo lường thời gian từ khi tin báo được xác nhận cho đến khi tin báo đó được chấp nhận. Nếu khoảng thời gian này bị vượt quá, hệ thống phải kích hoạt một chỉ báo cảnh báo. Nếu hệ thống có chức năng thiết lập được khoảng thời gian này thì chức năng này chỉ được phép thực hiện bởi người dùng có mức truy cập 3.

I.3.9.3 Nếu FAMS có chức năng ưu tiên mức độ đầu vào, phải có cơ chế giám sát khoảng thời gian từ khi tin báo được xác nhận đến khi được chấp nhận cho từng mức độ ưu tiên.

I.4 Thông tin cần hiển thị

I.4.1 Thông tin liên quan đến tin báo cần hiển thị

I.4.1.1 FAMS phải hiển thị các thông tin liên quan đến tin báo đã xác nhận nhằm hỗ trợ nhân viên vận hành tại FARC thực hiện hành động phù hợp. Thông tin này phải được hiển thị trước khi tin báo được chấp nhận, và có thể được truy xuất khi có yêu cầu.

I.4.1.2 Thông tin liên quan đến tin báo FAMS cung cấp bao gồm:

a) Danh tính của FDAS gửi tin báo, ít nhất phải bao gồm địa chỉ của cơ sở được giám sát;

b) Loại và/hoặc nội dung tin báo (ví dụ: báo cháy, báo lỗi..., dấu thời gian các sự kiện xảy ra);

c) Ngày và giờ FAMS xác nhận tin báo (chính xác đến từng giây);

d) Ngày và giờ tin báo được gửi bởi SPT (chính xác đến từng giây);

e) Mức độ ưu tiên của tin báo.

CHÚ THÍCH 1: Loại tin báo có thể được tích hợp trong nội dung tin báo.

CHÚ THÍCH 2: Các thông tin khác có thể được hiển thị, miễn là chúng không làm ảnh hưởng đến các thông tin chính cần hiển thị nêu trên.

I.4.1.3 Nội dung và cấu trúc của thông tin hiển thị phải được thống nhất giữa cơ sở, FARC và lực lượng chữa cháy.

I.4.2 Thông tin liên quan đến lỗi nhận được từ FDAS

Thông tin tối thiểu phải có trong tin báo lỗi:

a) Danh tính của FDAS gửi lỗi, ít nhất phải bao gồm địa chỉ của cơ sở được giám sát;

b) Loại lỗi (ví dụ: mất nguồn điện);

c) Sự kiện lỗi (ví dụ: lỗi nguồn điện chính);

d) Ngày và giờ sự kiện lỗi xảy ra.

I.4.3 Lỗi trong thiết bị hiển thị thông tin

Nếu trường hợp thiết bị hiển thị thông tin tại FARC bị lỗi hoàn toàn, dẫn đến mất khả năng thông tin cho nhân viên vận hành tại FARC thì FAMS không được xác nhận các tin báo mới đến và một lỗi phải được tạo ra và cảnh báo phải được kích hoạt.

I.5 Ghi nhận nhật ký

I.5.1 Tổng quan

I.5.1.1 Luồng thông tin của hệ thống FAMS bao gồm: Việc tạo lập và duy trì dữ liệu gốc (master data), xử lý các sự kiện, và truyền cảnh báo đến các hệ thống FAMS khác (nếu có) thông qua mô-đun liên kết

I.5.1.2 Thông tin có thể được FAMS xử lý tự động hoặc xử lý thủ công bởi nhân viên vận hành, hệ thống phải cho phép chuyển đổi linh hoạt giữa hai chế độ này. Trong quá trình xử lý, không được để xảy ra mất mát hoặc sai lệch thông tin.

I.5.1.3 Để đảm bảo nhất quán về luồng thông tin, FAMS phải có khả năng tạo ra các nhật ký theo chuẩn định dạng cố định. Các loại nhật ký này bao gồm: Nhật ký dữ liệu gốc (M-Log); Nhật ký dữ liệu sự kiện (E-Log), và nếu có, bao gồm cả nhật ký mô-đun liên kết (J-Log).

I.5.1.4 Dữ liệu đã được ghi phải được bảo vệ chống lại việc xóa nhầm hoặc cố ý, cũng như chống ghi đè. Dữ liệu lịch sử phải có thể truy xuất theo yêu cầu.

I.5.1.5 Việc thay đổi (thêm mới, chỉnh sửa, hoặc xóa) dữ liệu làm nguồn tạo ra các nhật ký chỉ được phép thay đổi thông qua các chức năng do FAMS cung cấp và mọi thay đổi dữ liệu làm nguồn đó phải có khả năng truy vết.

I.5.2 Dấu thời gian cho nhật ký

I.5.2.1 FAMS phải tạo ra dấu thời gian cần thiết (với độ chính xác đến giây) và lưu trữ đầy đủ để có thể truy xuất phục vụ việc kiểm tra, đánh giá.

I.5.2.2 Dấu thời gian trong các mục ghi nhật ký phải phản ánh thời điểm hoàn thành của mỗi thao tác đã được ghi lại. Dấu thời gian phải được thể hiện theo UTC với độ phân giải chính xác tối thiểu là 1 s.

I.5.2.3 FAMS có tích hợp giao diện kết nối với RCT (I_{RCT}) phải ghi lại các dấu thời gian T_{RCT} và T_{tn}, và được lưu lại để kiểm tra, đánh giá.

I.5.2.4 Đối với các sự kiện không được kích hoạt bởi tin báo đến qua giao diện I_{RCT} thì thời điểm tạo sự kiện sẽ được sử dụng làm T_{RCT}. Trong trường hợp này, thời điểm FAMS bắt đầu xử lý hoặc nhân viên vận hành FARC bắt đầu thao tác sẽ được sử dụng làm T_{tn}.

I.5.3 Nhật ký dữ liệu gốc (Nhật ký M1)

I.5.3.1 Dữ liệu gốc được trao đổi với các hệ thống con, đối tượng và quy trình phải được ghi lại trong nhật ký M1.

I.5.3.2 Tất cả các bản ghi mới và thay đổi dữ liệu phải được lưu lại theo cách cho phép xác định rõ thời điểm xảy ra thay đổi và tác nhân (người hoặc hệ thống tự động) thực hiện thay đổi. FAMS phải có khả năng khôi phục lại trạng thái của dữ liệu gốc tại bất kỳ thời điểm nào trong khoảng thời gian dữ liệu được lưu giữ.

I.5.4 Nhật ký sự kiện

I.5.4.1 Nhật ký sự kiện E1

I.5.4.1.1 Nhật ký sự kiện E1 phải được sử dụng để ghi lại dữ liệu đầu vào (dữ liệu thô) nhận được thông qua giao diện I_{RCT}. Nhật ký này cũng có thể được sử dụng để lưu dữ liệu từ các giao diện và mô-đun khác.

I.5.4.1.2 Trong nhật ký sự kiện E1, dữ liệu gốc thô (dữ liệu vừa được tiếp nhận, chưa xử lý) nhận được sẽ được ghi lại cùng với mã số định danh nhật ký E1 (E1-ID Number) và dấu thời gian của FAMS tại thời điểm ghi nhận. Dấu thời gian này tương ứng với T_{RCT}.

I.5.4.2 Nhật ký sự kiện E2

I.5.4.2.1 Nhật ký sự kiện E2 biểu thị dữ liệu đã được xử lý ở định dạng cụ thể của FAMS, bao gồm:

a) Mã số định danh nhật ký E2 (E2-ID Number), bao gồm cả liên kết đến một hoặc nhiều bản ghi nhật ký E1.

b) Dấu thời gian của FAMS ($T_{Log\ E2}$) tại thời điểm ghi nhận bản ghi này.

I.5.4.2.2 Nhiều bản ghi E1 có thể tổng hợp thành một bản ghi E2, hoặc một bản ghi E1 có thể chuyển thành nhiều bản ghi E2.

I.5.4.3 Nhật ký sự kiện E3

I.5.4.3.1 Nhật ký sự kiện E3 thể hiện kết quả hợp nhất các bản ghi nhật ký E2, bao gồm mã định danh đối tượng duy nhất và mã định danh của sự kiện liên quan từ dữ liệu gốc hoặc từ thông tin định danh của sự kiện nội bộ.

1.5.4.3.2 Nhật ký sự kiện E3 cũng phải bao gồm mã số định danh nhật ký sự kiện E3 (E3-ID Number) và dấu thời gian của FAMS ($T_{Log\ E3}$) tại thời điểm ghi nhận bản ghi.

I.5.4.3.3 Nhiều bản ghi E2 có thể được tổng hợp thành một bản ghi E3 hoặc một bản ghi E2 có thể được phân tách để tạo thành nhiều bản ghi E3.

I.5.4.3.4 Nếu một bản ghi E2 không thể liên kết với đối tượng hoặc sự kiện cụ thể (ví dụ: do thiếu hoặc dữ liệu gốc không chính xác), thì vẫn phải được đưa vào nhật ký E3, mặc dù không có tham chiếu đầy đủ.

I.5.4.3.5 Các sự kiện nội bộ do FAMS tạo ra (ví dụ sự kiện khi không nhận được thông báo định kỳ) hoặc sự kiện do nhân viên vận hành FARC tạo ra, cũng phải được ghi nhận trong nhật ký sự kiện này.

I.5.4.4 Nhật ký sự kiện E4

I.5.4.4.1 Nhật ký sự kiện E4 thể hiện kết quả của các hành động và phản hồi do FAMS và/hoặc nhân viên vận hành FARC thực hiện trong quá trình xử lý các bản ghi E3.

I.5.4.4.2 Bản ghi E4 cũng bao gồm mã số định danh nhật ký sự kiện E4 (E4-ID Number) và dấu thời gian ghi nhận của FAMS (TLog E4) tại thời điểm ghi nhận bản ghi.

I.5.4.4.3 Nhiều bản ghi E3 có thể được tổng hợp thành một bản ghi E4, hoặc một bản ghi E3 có thể được phân tách thành nhiều bản ghi E4.

I.5.4.5 Lỗi trong nhật ký

Trong trường hợp nhật ký gặp lỗi, một chỉ báo cảnh báo phải được kích hoạt trong vòng 5 s sau khi RCT gửi một tin nhắn đến FAMS nhưng không thể được ghi lại do lỗi chức năng ghi nhật ký.

I.5.5 Mức truy cập

I.5.5.1 FAMS phải có biện pháp để hạn chế truy cập vào các chức năng của hệ thống.

I.5.5.2 Nhà sản xuất FAMS phải quy định rõ biện pháp để kiểm soát truy cập (ví dụ: khóa vật lý hoặc mật khẩu logic), cũng như các chức năng có thể truy cập tại mỗi mức truy cập

I.5.5.3 Quyền truy cập vào các chức năng của FAMS phải được chia thành tối thiểu bốn mức độ như sau:

a) Mức truy cập 1: không yêu cầu xác thực;

b) Mức truy cập 2: cho phép vận hành FAMS (ví dụ: chấp nhận tin báo);

c) Mức truy cập 3: cho phép cấu hình hoặc chỉnh sửa cấu hình FAMS (ví dụ: tắt chỉ báo cảnh báo hoặc thiết lập mức đô ưu tiên đầu vào);

d) Mức truy cập 4: cho phép truy cập và thực hiện thay đổi phần cứng hoặc phần mềm của FAMS (ví dụ: các sửa đổi do nhà sản xuất FAMS thực hiện).

I.5.5.4 Việc truy cập ở mức 4 phải bị ngăn chặn cho đến khi quyền truy cập ở mức 3 đã được cho phép.

CHÚ THÍCH: Điều này có nghĩa rằng người dùng không được phép truy cập trực tiếp vào mức truy cập 4 từ trạng thái chưa đăng nhập hoặc từ mức truy cập 1, 2 mà phải được cấp quyền ở mức 3 trước, rồi mới mở khóa để truy cập vào mức 4.

I.5.5.5 Mỗi mức truy cập có thể được chia thành nhiều mức con, các mức con này phải được mô tả trong tài liệu của nhà sản xuất FAMS.

I.5.5.6 Việc vận hành FAMS yêu cầu mỗi người dùng phải đăng nhập ở mức truy cập phù hợp và đăng xuất khi kết thúc phiên làm việc. Việc đăng nhập, đăng xuất và mọi thay đổi mật khẩu (nếu có) phải được ghi lại trong nhật ký hệ thống.

I.5.5.7 Ở mức truy cập 3, FAMS phải có phương pháp để xác định người dùng và các mức truy cập liên quan của họ.

I.5.5.8 FAMS phải có công cụ để chỉnh sửa thông tin người dùng, phân quyền truy cập và thay đổi mật khẩu. Việc thay đổi mật khẩu chỉ được phép thực hiện bởi chính người dùng đó hoặc người dùng có quyền truy cập mức 4.

I.5.6 Truy cập cơ sở dữ liệu

I.5.6.1 Việc chỉnh sửa cơ sở dữ liệu có thể được thực hiện tại chỗ và/hoặc từ xa, với điều kiện người dùng có quyền truy cập ở mức 3.

I.5.6.2 Khi RCT được sử dụng để kết nối với SPT thì không được phép truy cập từ xa vào cơ sở dữ liệu của FAMS thông qua RQT này.

I.5.7 Truy cập vào FAMS

Quyền truy cập vào các chức năng chấp nhận tin báo và hiển thị thông tin phải được giới hạn ở mức truy cập 2.

I.5.8 Truy cập vào dữ liệu cấu hình của FAMS

I.5.8.1 Nếu FAMS có chứa dữ liệu cấu hình, việc truy cập vào dữ liệu này phải được ủy quyền thông qua các mức truy cập phù hợp.

I.5.8.2 FAMS phải có biện pháp để cho phép xem và chỉnh sửa dữ liệu cấu hình hệ thống. Việc xem dữ liệu cấu hình yêu cầu quyền truy cập mức 2. Việc chỉnh sửa dữ liệu cấu hình yêu cầu quyền truy cập mức 3. Tất cả các thay đổi đối với dữ liệu cấu hình phải được ghi lại trong nhật ký hệ thống (ví dụ như thiết lập hoặc thay, đổi mật khẩu).

I.5.9 Truy cập vào dữ liệu nhật ký

FAMS phải cung cấp biện pháp để truy cập vào dữ liệu nhật ký. Việc truy cập dữ liệu nhật ký để sao lưu phục vụ lưu trữ dài hạn phải bị giới hạn ở mức truy cập 3.

I.6 Giám sát kết nối với RCT

I.6.1 FAMS phải giám sát kết nối với RCT. Phương thức giám sát và loại lỗi cần phát hiện phải được mô tả trong tài liệu của nhà sản xuất (ví dụ: ngắn mạch, hở mạch, mất kết nối, v.v.) nhưng ít nhất, FAMS phải phát hiện và nhận biết được sự gián đoạn vật lý trong kết nối.

CHÚ THÍCH: Sự gián đoạn vật lý trong kết nối là tình trạng mà kết nối giữa FAMS và RCT bị mất do lỗi xảy ra ở phần cứng (ví dụ đứt, hỏng cáp; mất điện; cổng giao tiếp, card mạng hỏng; các thiết bị như mạng bên thứ ba hỏng ....) khiến không có tín hiệu hoặc dữ liệu nào có thể được truyền qua.

I.6.2 Trong trường hợp kết nối giữa FAMS và RCT bị lỗi:

- Thông tin lỗi phải được tạo ra và hiển thị trong vòng 10 s kể từ khi xuất hiện lỗi;

- Chỉ báo cảnh báo lỗi phải được kích hoạt trong vòng 10 s kể từ khi xuất hiện lỗi.

- FAMS không được xác nhận bất kỳ tin báo nào từ RCT có lỗi kết nối với FAMS kể từ khi xảy ra lỗi cho đến khi lỗi được khắc phục.

Phụ lục K

(Tham khảo)

Bảng K.1 - Quy trình vận hành trung tâm tiếp nhận báo cháy

STT	Nội dung	Yêu cầu
1	Tạo, sửa đổi và hủy tài khoản của cơ sở được giám sát	Quy trình phải mô tả cách thức lưu trữ và sửa đổi dữ liệu gốc như quy định tại 6.1.5; 6.1.6.
2	Xử lý tin báo	Quy trình phải mô tả trình tự xử lý tin báo tại FARC, bao gồm: Tiếp nhận, phân tích nội dung, cung cấp thông tin cho nhân viên vận hành (T_{tn}), thực hiện hành động đầu tiên bởi nhân viên vận hành hoặc hệ thống FAMS ($T_{hđ}$) theo quy trình đã định trước (xem hình 1).
3	Liên lạc với các lực lượng chữa cháy, cơ sở và/ hoặc các lực lượng khác liên quan	Quy trình phải bao gồm kế hoạch, thỏa thuận hoặc yêu cầu giữa FARC với các lực lượng khác như lực lượng chữa cháy, cơ sở và/ hoặc các lực lượng khác liên quan.
4	Dịch vụ do FARC cung cấp	Quy trình phải liệt kê tất cả dịch vụ do FARC cung cấp, bao gồm cả chất lượng, hiệu năng kèm theo.
5	Lọc tin báo cháy	Khi quy trình xử lý tin báo áp dụng lọc tin báo cháy, quy trình phải mô tả phương pháp, cách thức thực hiện.
6	Gia tăng đột biến tín hiệu báo cháy hoặc báo lỗi	Quy trình phải mô tả các biện pháp dự phòng để xử lý tình trạng gia tăng bất thường của tín hiệu báo cháy hoặc báo lỗi (ví dụ báo cháy giả hoặc báo lỗi do yếu tố môi trường, thời tiết; các sự cố kết nối mạng...).
7	Lỗi FATP	Quy trình phải mô tả cách phát hiện, phân loại và xử lý các lỗi FATP, bao gồm cả chỉ số đánh giá hiệu quả xử lý và khôi phục.
8	Kiểm soát để duy trì chất lượng dịch vụ	Quy trình phải có biện pháp kiểm soát nhằm ngăn chặn sự sụt giảm chất lượng xử lý của FARC với các sự cố tại cơ sở, gồm yếu tố kỹ thuật cũng như con người.
9	Lắp đặt, bảo trì, bảo vệ, tháo gỡ và tái sử dụng tài sản thuộc quyền kiểm soát của FARC	Quy trình phải quy định ai được phép phê duyệt, thực hiện việc lắp đặt, duy trì, tháo gỡ tài sản. Phải xem xét các rủi ro liên quan đến dữ liệu và phần mềm bản quyền lắp trong tài sản đó. Đồng thời có biện pháp phù hợp bảo vệ các tài sản không có người trông coi.
10	Giám sát và kiểm tra thiết bị	Để đảm bảo FARC hoạt động chính xác, cần thực hiện giám sát và kiểm tra định kỳ tất cả thiết bị và ghi lại kết quả
11	Xử lý lỗi và báo cáo lỗi	- Quy trình phải mô tả cách thức FARC xử lý và ghi nhận các lỗi kỹ thuật ảnh hưởng đến tiếp nhận và truyền tin, bao gồm cả nguồn điện. Tối thiểu phải đáp ứng: + Bất kỳ thiết bị nào liên quan đến việc tiếp nhận, hiển thị hoặc truyền tin báo cháy hoặc báo lỗi (bao gồm nguồn điện) phải có phương án dự phòng có thể được kích hoạt tự động hoặc bởi nhân viên vận hành trong vòng một giờ kể từ khi lỗi được phát hiện. + Việc sửa chữa hoặc thay thế thiết bị lỗi phải bắt đầu trong vòng 15 phút kể từ thời điểm phát hiện lỗi. + Mọi lỗi phải được ghi nhận bằng tay hoặc tự động vào sổ nhật ký lỗi. - Tỷ lệ hoạt động hàng tháng của FARC phải được thể hiện bằng phần trăm thời gian mà các thành phần chức năng xử lý tin báo hoạt động theo tiêu chuẩn này. Các thành phần chức năng bao gồm tất cả thiết bị tham gia vào việc tiếp nhận và xử lý tin báo cháy, báo lỗi; FAMS cùng với phần cứng, phần mềm và các thành phần mạng cần thiết. CHÚ THÍCH: Nếu các thành phần chức năng có cấu hình nhân đôi (dự phòng) để cung cấp tính dự phòng, đảm bảo rằng lỗi của một thành phần riêng lẻ không ảnh hưởng đến việc tiếp nhận hoặc hiển thị tin báo, thì tỷ lệ hoạt động vẫn được coi là 100 %.
12	Quản lý thông tin	Quy trình phải mô tả rõ cách thức quản lý toàn bộ dữ liệu trong hệ thống, bao gồm việc duy trì, lưu trữ, tổ chức, chỉnh sửa và truy xuất. Quy trình vận hành cần nêu cụ thể cách dữ liệu gốc của từng cơ sở được giám sát liên kết với các thành phần tiếp nhận tin báo, nhằm bảo đảm việc tự động hiển thị cảnh báo và lưu giữ các sự kiện vận hành liên quan đến từng khách hàng. Các quy trình bổ sung cần quy định rõ cách bảo vệ, xử lý và lưu giữ dữ liệu an toàn. Cần có biện pháp kiểm soát nhằm ngăn chặn mất dữ liệu,

		hư hỏng, giả mạo, truy cập trái phép hoặc rò rỉ thông tin, bất kể do lỗi vô tình hay hành vi cố ý. Các biện pháp này phải đáp ứng các quy định pháp lý hiện hành và các cam kết trong thỏa thuận. Đối với mỗi hệ thống FDAS được kết nối vào trung tâm, phải thiết lập một hồ sơ riêng biệt, có mã nhận dạng duy nhất, trong đó lưu thông tin cấu hình, dữ liệu liên quan và các hướng dẫn xử lý. Đồng thời, cần có một hồ sơ lịch sử riêng (hoặc tích hợp trong cùng hồ sơ) để ghi lại đầy đủ mọi hoạt động của người vận hành có liên quan đến hệ thống đó.
13	Sao lưu dữ liệu	Quy trình phải mô tả cách sao lưu toàn bộ dữ liệu khách hàng và dữ liệu hệ thống, cũng như cách kiểm tra định kỳ để đảm bảo khả năng truy xuất và độ tin cậy của bản sao lưu. Nếu FARC hoạt động song song với một FARC khác, dữ liệu khách hàng phải sẵn có tại cả hai trung tâm.
14	Bảo mật và phân loại thông tin	Quy trình phải quy định cách đảm bảo tính bảo mật của dữ liệu được truy cập bởi các cá nhân trong FARC
15	Quan hệ với các nhà cung cấp thiết yếu (FATSP, nhà cung cấp hạ tầng mạng, các đơn vị cung cấp dịch vụ bảo trì, phần mềm, dữ liệu...)	Quy trình phải mô tả cách FARC làm việc với các nhà cung cấp thiết yếu. Mỗi nhà cung cấp phải có thỏa thuận riêng kèm quy trình cụ thể được thỏa thuận. FARC phải giám sát và đánh giá hiệu quả hoạt động của nhà cung cấp theo các quy trình đã thống nhất, định kỳ không quá 1 năm/lần.
16	Quy trình hành chính	Quy trình phải làm rõ cách các hoạt động vận hành của FARC được kết nối với quy trình hành chính như: bán hàng, quản lý thỏa thuận khách hàng/nhà cung cấp, lập hóa đơn... nhằm đảm bảo tính nhất quán xuyên suốt.
17	Kiểm soát truy cập vật lý	Quy trình phải mô tả cách quyền truy cập và thoát khỏi FARC được kiểm soát. Quy trình phải xác định phương thức xác minh danh tính của những người yêu cầu truy cập.
18	Truy cập từ xa	Quy trình phải mô tả cách kiểm soát truy cập từ xa vào bất kỳ hệ thống nào trong FARC cũng như vào thiết bị xử lý dữ liệu từ xa. Việc truy cập phải được ghi nhận đầy đủ thông qua cơ chế đăng nhập/đăng xuất, bao gồm: thời gian truy cập, thông tin xác thực, người thực hiện và các hành động đã thực hiện. Truy cập từ xa chỉ được phép thực hiện khi có sự cho phép từ FARC.
19	Duy trì hoạt động và xử lý tình huống khẩn cấp	Quy trình phải bao gồm kế hoạch bảo đảm liên tục hoạt động và phục hồi sau sự cố. Kế hoạch phải mô tả chi tiết cách khôi phục dịch vụ sau tình huống khẩn cấp. FARC phải rà soát kế hoạch này định kỳ 6 tháng/lần. Nhân viên phải được đào tạo lại về các quy trình vận hành và xử lý tình huống khẩn cấp để đối phó với các sự kiện gián đoạn dịch vụ, bao gồm: a) Quy trình phản ứng khẩn cấp phải được thỏa thuận với các đơn vị liên quan, nhằm duy trì chức năng giám sát của FARC trong khi sự cố đang được xử lý. b) Nếu FARC bị vô hiệu hóa hoàn toàn, phải có một quy trình vận hành khẩn cấp để xử lý tình huống này (ví dụ: chuyển giao dịch vụ sang FARC khác, thông báo cho khách hàng và đối tác).
20	Sơ tán khẩn cấp và khôi phục hoạt động	Quy trình phải mô tả cách thực hiện sơ tán một phần hoặc toàn bộ FARC, bao gồm các hành động cần thực hiện để quay lại và/hoặc khôi phục hoạt động sau khi sơ tán.
21	Lối vào khẩn cấp	Trong trường hợp việc ra vào FARC được kiểm soát bởi nhân viên vận hành bên trong FARC, thì cần có thiết bị hoặc quy trình dự phòng cho phép tiếp cận FARC mà không cần sự hỗ trợ từ bên trong. Bất kỳ chìa khóa, mã số hoặc thẻ từ nào dùng để mở lối vào này phải được lưu trữ tại vị trí an toàn, ví dụ như trong két sắt, và chỉ những người được chỉ định trong danh sách mới có quyền truy cập. Cơ chế lối vào này không được sử dụng như phương thức ra vào thông thường, mà chỉ nên được dùng trong các trường hợp đặc biệt,

		chẳng hạn như tình huống khẩn cấp. Tất cả nhân viên phải được hướng dẫn và đào tạo về các quy trình khẩn cấp định kỳ không quá sáu tháng một lần và quá trình đào tạo này phải được ghi nhận lại.
22	Chỉ số đánh giá hiệu quả hoạt động	Quy trình phải mô tả cách thức xây dựng số liệu thống kê về hiệu quả hoạt động của FARC và cung cấp để chứng minh việc thực hiện đầy đủ các dịch vụ đã được hợp đồng. Các chỉ số này phải bao gồm: a) Mức độ hoàn thành mỗi dịch vụ được cung cấp theo thỏa thuận với khách hàng. b) Hiệu năng xử lý tin báo cháy. c) Tần suất, thời gian khôi phục các lỗi FATP.

Thư mục tài liệu tham khảo

[1] TCVN 7563 (ISO/IEC 2382) (tất cả các phần), *Công nghệ thông tin - từ vựng*

[2] TCVN 7568-14 (ISO 7240-14) Hệ *thống báo cháy - Phần 14: Thiết kế, lắp đặt các hệ thống báo cháy cho nhà và công trình*

[3] TCVN 7568-21 (ISO 7240-21) *Hệ thống báo cháy - Phần 21: Thiết bị định tuyến*

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

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

[6] EN 54-21: 2006 *Fire detection and fire alarm systems - Part 21: Alarm transmission and fault warning routing equipment* (Hệ thống phát hiện cháy và báo cháy - Phần 21: Thiết bị định tuyến cảnh báo sự cố và truyền tín hiệu báo động)

[7] BSEN 50136-1 *Alarm systems - Alarm transmission systems and equipment - Part 1: General requirements for alarm transmission systems* (Hệ thống báo động - Hệ thống và thiết bị truyền tín hiệu báo động - Phần 1: Yêu cầu chung đối với hệ thống truyền tín hiệu báo động)

[8] BSEN 50136-2 *Alarm systems - Alarm transmission systems and equipment - Part 2: Requirements for Supervised Premises Transceiver (SPT)* (Hệ thống báo động - Hệ thống và thiết bị truyền tín hiệu báo động - Phần 2: Yêu cầu đối với Thiết bị thu phát tại cơ sở được giám sát (SPT))

[9] BSEN 50136-3 *Alarm systems - Alarm transmission systems and equipment - Part 3: Requirements for Receiving Centre Transceiver (RCT)* (Hệ thống báo động - Hệ thống và thiết bị truyền tín hiệu báo động - Phần 3: Yêu cầu đối với Thiết bị thu phát tại trung tâm tiếp nhận (RCT))

[10] EN 50518 *Monitoring and alarm receiving centre* (Trung tâm giám sát và tiếp nhận báo động)

[11] BS 9518 *Processing of alarm signals by an alarm receiving centre - Code of practice* (Xử lý tín hiệu báo động tại trung tâm tiếp nhận báo động - Quy phạm thực hành)

[12] NFPA 72 *National fire alarm and singaling code (Quy phạm quốc gia về hệ thống báo cháy và tín hiệu)*

[13] CLC/TS 50136-7 *Alarm systems - Alarm transmission systems and equipment - Part 7: Application guidelines* (Hệ thống báo động - Hệ thống và thiết bị truyền tín hiệu báo động - Phần 7: Hướng dẫn áp dụng)

MỤC LỤC