SLOVENSKI STANDARD
SIST-TS CLC/TS 50134-9:2018

01-november-2018

Alarmni sistemi - Socialni alarmni sistemi - 9. del: Komunikacijski protokoli IP

Alarm systems - Social alarm systems - Part 9: IP Communications Protocol

Systèmes d'alarme - Systèmes d'alarme sociale - Partie 9: Protocole de communication IP

Ta slovenski standard je istoveten z: **CLC/TS 50134-9:2018**

ICS:

13.320 Alarmni in opozorilni sistemi Alarm and warning systems

SIST-TS CLC/TS 50134-9:2018 **en**

TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

CLC/TS 50134-9

September 2018

ICS 13.320; 35.240.99

English Version

Alarm systems - Social alarm systems - Part 9: IP Communications Protocol

Systèmes d'alarme - Systèmes d'alarme sociale - Partie 9: Protocole de communication IP

Alarmanlagen - Personen-Hilferufanlagen - Teil 9: IP Übertragungsprotokoll

This Technical Specification was approved by CENELEC on 2018-05-28.

CENELEC members are required to announce the existence of this TS in the same way as for an EN and to make the TS available promptly at national level in an appropriate form. It is permissible to keep conflicting national standards in force.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

Ref. No. CLC/TS 50134-9:2018 E

Contents

Page

European foreword

This document (CLC/TS 50134-9:2018) has been prepared by CLC/TC 79 “Alarm systems”.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC shall not be held responsible for identifying any or all such patent rights.

EN 50134 consists of the following parts, under the general title *Alarm systems — Social alarm systems*:

— *Part 1: System requirements*;

— *Part 2: Trigger devices*;

— *Part 3: Local unit and controller*;

— *Part 5: Interconnections and communications*;

— *Part 7: Application guidelines*;

— *Part 9: IP Communications Protocol* [the present Technical Specification].

Annexes which are designated “informative” are given for information only.

Introduction

As telecommunication operators continue to migrate towards Next Generation Networks they are increasingly converging voice traffic onto their IP infrastructures which may have an adverse impact on the reliability of in-call, tone based protocols.

The impact differs per country but is rapidly increasing across Europe. In addition, cellular technology is increasingly used next to broadband, cable and fibre solutions.

This Technical Specification defines the IP communications protocol for social alarms, optimized for stand-alone usage. The majority of current social alarms usage is stand-alone within the home and not related to other alarm systems. The combination of social alarms with other types of alarm systems is pending for a future version of this standard.

1 Scope

This Technical Specification specifies a protocol for point-to-point transmission of alarms, faults, control signals and communications monitoring, between a Local Unit and Controller and an Alarm Receiving Centre using the Internet protocol (IP). The protocol is intended for use over any network that supports the transmission of IP data with sufficient quality of service to support VoIP or a separate voice channel.

The Alarm Protocol is defined as an XML scheme including the alarm types, codes and necessary additional information.

The alarm protocol is an application layer protocol using another Internet Protocol as a transport protocol to handle addressing and transport functions. The transport protocol initially defined in this Technical Specification is SIP (Session Initiation Protocol).

The system performance characteristics for alarm transmission are specified in EN 50134-5. The performance characteristics of the Local Unit and Controller are expected to comply with the requirements of its associated alarm system standard and to apply for the transmission of social alarms.

The protocols described in this standard are based on the SS 91100:2014 SCAIP standard [7] and defined to enable backwards compatibility with existing products based on the SCAIP standard.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

EN 50134–1, *Alarm systems — Social alarm systems — Part 1: System requirements*

ISO 8601, *Data elements and interchange formats — Information interchange — Representation of dates and times*

ITU X509, *Information technology — Open Systems Interconnection — The Directory: Public-key and attribute certificate frameworks*

RFC 2119, *Key words for use in RFCs to Indicate Requirement Levels*

[HTTP-AUTH] RFC 2617, *HTTP Authentication: Basic and Digest Access Authentication*

[SIP] RFC 3261, *SIP: Session Initiation Protocol*

[SDP] RFC 3264, *An Offer/Answer Model with the Session Description Protocol (SDP)*

[SIP-IM] RFC 3428, *Session Initiation Protocol (SIP) Extension for Instant Messaging*

[RTP] RFC 3550, *RTP: A Transport Protocol for Real-Time Applications*

[SRTP] RFC 3711, *The Secure Real-time Transport Protocol (SRTP)*

[SDP-SEC] RFC 4568, *Session Description Protocol (SDP) - Security Descriptions for Media Streams*

[RTP-DTMF] RFC 4733, *RTP Payload for DTMF Digits, Telephony Tones, and Telephony Signals*

[ICE] RFC 5245, *Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols*

[STUN] RFC 5389, *Session Traversal Utilities for NAT (STUN)*

[SRTP-DTLS] RFC 5764, *Datagram Transport Layer Security (DTLS) Extension to Establish Keys for the Secure Real-time Transport Protocol (SRTP)*

[TURN] RFC 5766, *Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)*

[SIP-ICE] RFC 5768, *Indicating Support for Interactive Connectivity Establishment (ICE) in the Session Initiation Protocol (SIP)*

RFC 5870, *A Uniform Resource Identifier for Geographic Locations ('geo' URI)*

[SIP-NAT] RFC 6314, *NAT Traversal Practices for Client-Server SIP*

G.711 (11/88), *Pulse code modulation (PCM) of voice frequencies*

G.729 (06/12), *Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear prediction (CS-ACELP)*

3 Terms, definitions and abbreviations

3.1 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

3.1
alarm receiver
alarm receiving centre
system part which provides facilities for communication with a number of controllers, and providing the alarm receiving and information processing system as an interface to the alarm recipient

3.2
codec
device capable of encoding and decoding a digital data stream or signal

3.3
controller
alarm sender
interface between one or more Local Units and the alarm transmission system or alarm recipient

3.4
heartbeat
periodic event generated by hardware or software to indicate normal operation or to synchronize parts of a system

3.5
in-band signalling
sending of control information within the same band or channel used for voice

3.6
interconnections
transmission system that provides the communication between trigger devices and local unit and controller

3.7
Local Unit and Controller
interface between the user and the controller which enables two-way speech

3.8
multimedia
media and content that use a combination of different content forms as text, audio, still images, animation, video or interactivity

3.9
polling
sampling of a device to synchronize an activity

3.10
protocol
system of digital rules for message exchange within or between computers

3.11
social alarm system
telecare system
system providing 24 h facilities for alarm triggering, identification, signal transmission, alarm reception, two-way speech communication, reassurance and assistance, for use by persons considered to be at risk

3.2 Abbreviations

Abbreviation	Definition
ARC	Alarm Receiving Centre
ASCII	American Standard Code for Information Interchange
GGA	Global Positioning System Fix Data
GPS	Global Positioning System
GSM	Global System for Mobile Communications
IP	Internet Protocol
ISO	International Organization for Standardization
LUC	Local Unit and Controller
NMEA	National Marine Electronics Association
POTS	Plain Old Telephone Service
RFC	Request for Comments
RTP	Real-time Transport Protocol
SRTP	Secure Real-time Transport Protocol
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SIP-PP	Session Initiation Protocol, Peer-to-peer.
TLS	Transport Layer Security
UCS	Universal Character Set
UDP	User Datagram Protocol
UTF	UCS Transformation Formats
XML	eXtensible Markup Language
URI	Uniform Resource Identifier

Abbreviation	Definition
SCAIP	Social Care Alarm Internet Protocol
NGN	Next Generation Network, a packet-based network able to provide services including Telecommunication Services (such as voice) and able to make use of multiple broadband, QoS-enabled transport technologies and in which service-related functions are independent from underlying transport-related technologies.

4 Social Alarm transmission network architecture

4.1 General

The network architecture assumed by this standard as shown in Figure 1 is the existence of an all IP network used for both the alarm communication protocol and voice, or the existence of an IP network for the alarm communication protocol and a separate voice path outside of the IP network. The separate voice network can be provided by cellular, analog POTS, broadband cable or VoIP operator infrastructure or a combination of these.

In addition, in the second case the IP network may not be available while a voice session is in progress (e.g. when 2G/2.5G modems are used in the LUC). Note that the second case is technology agnostic with respect to the technology between LUC and voice network and the technology between ARC and voice network other than the requirement that LUC and ARC are addressable via E.164 addressing.

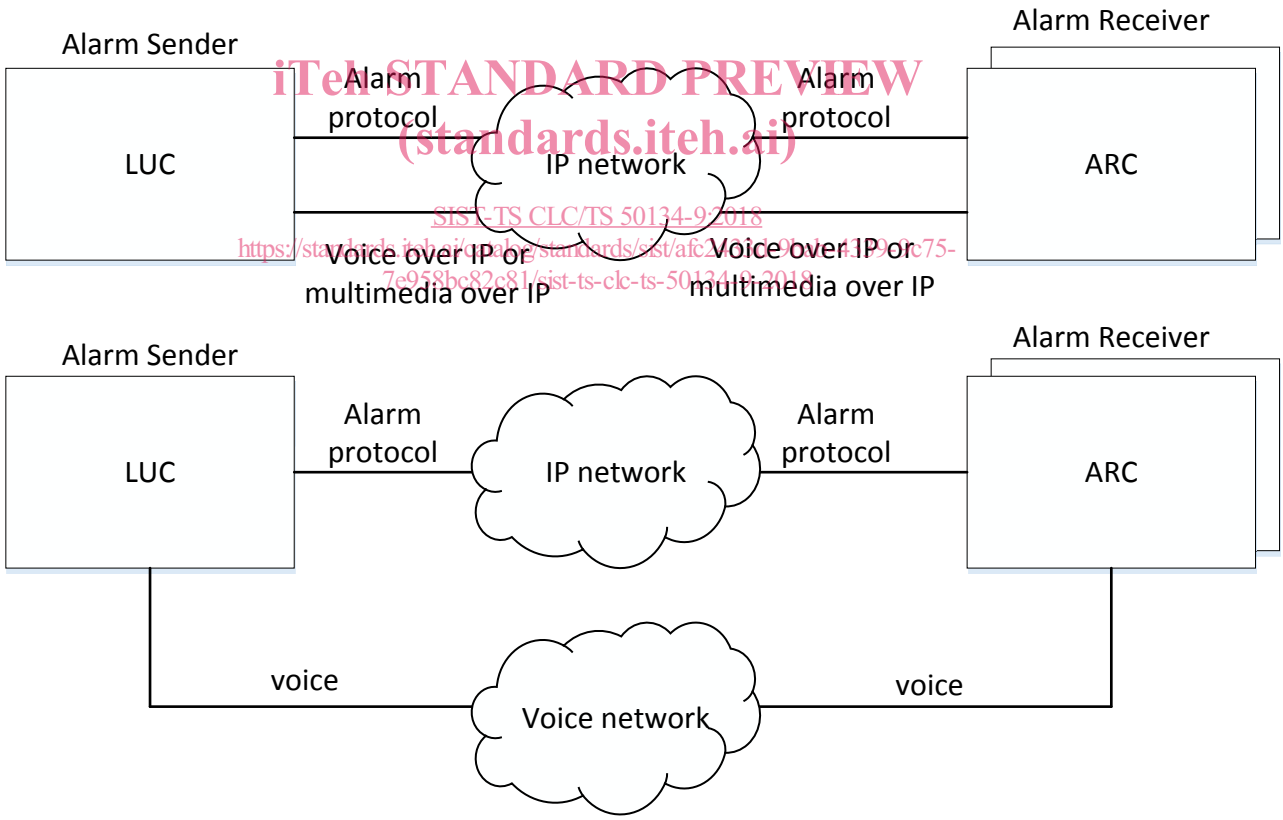

Figure 1 — Network architecture options

The protocol allows for a LUC to communicate to multiple ARCs. The mechanisms for ensuring availability of an ARC and ensuring the LUC communicates to the correct ARC are not part of this standard, but could consist of, for example, global load balancing, DNS, SIP proxies as part of the IP network, or use of the status code in the message response indicating to the LUC to contact the another ARC.

In addition, there may be constraints in the IP network on the reachability of the LUC from the ARC due to the presence of an on premise NAT router or firewall.

4.2 Alarm and status messages

4.2.1 General

Alarm and status messages shall use SIP messaging [SIP-IM].

4.2.2 Authentication

The application layer protocol shall support authentication on a per connection basis, at least the same level of encryption and authentication mechanisms as SIP. Authentication shall be either user specific, where each alarm sender logs in on a separate account or group specific, where all alarm senders log in on a common account.

The authentication mechanism shall support HTTP Digest authentication.

Alarm receivers shall only accept and process messages from authenticated, and thus authorized, alarm senders. The LUC shall authenticate towards the ARC using HTTP digest authentication.

4.2.3 Encryption

The LUC and the ARC shall support encryption.

The LUC shall not transmit personal or sensitive information over an unsecure connection without encryption.

The LUC and ARC shall support secure SIP over unsecure connections.

Personal and Sensitive data are only allowed to be transmitted over secure SIP.

The ARC shall present a valid ITU X509 certificate.

LUC shall verify the identity of the server certificate using a local Root CA Certificate

LUC to ARC SIP session shall be encrypted with TLS V1.2 or higher.

LUC to ARC SIP session shall use cryptographic algorithms AES-128 encryption minimum.

NOTE The management of certificates and the behaviour when certificates are invalid are out of scope of this standard.

4.3 Voice / multimedia over IP implementation

Voice / multimedia channels over the IP network shall use SIP [SIP], SDP [SDP] and RTP [RTP].

LUC to ARC voice session shall support codec G.711 (a-law) or G.729 minimum.

The LUC shall support firewall traversal for VoIP and SIP using ICE [STUN], TURN [TURN], ICE for SIP [SIP-ICE] and NAT traversal for SIP [SIP-NAT].

The LUC and the ARC shall support secure communication through the use of TLS. The need for a secure connection is indicated by the use of a “sips:” URI as the destination for SIP. This also indicates the LUC and ARC shall use SRTP [SRTP] for the voice channel. The LUC and ARC shall support [SDP-SEC] to negotiate a secure voice channel.

LUC to ARC voice session shall be encrypted with SRTP using AES-128 encryption minimum

NOTE Whether secure communications need to be used is determined by the organization deploying the social alarm system.

4.4 Separate voice network

When the voice channel is set up out of band using a different technology such as a cellular network, a Next Generation Network (NGN) or an analog POTS, signalling and voice channel occur outside of the IP network. The voice channel in this case shall be able to terminate on the POTS or a NGN with voice functionality

supporting E.164 phone numbers at the ARC, so that ARC does not need special connectivity other than to the POTS or NGN. If the LUC supports call back, it shall be possible to call to the LUC using an E.164 phone number, which may be over cellular, NGN or analog POTS.

Some functions should be controlled by single DTMF codes from the alarm receiver to enable a basic control facility when the use of the voice channel results in loss of IP connectivity (e.g. 2G/2.5G cellular connectivity).

NOTE The alarm receiver of the Message Request might or might not be the same as the alarm receiver of the voice or multimedia communication. The alarm sender might be able to connect to multiple alarm receivers for different events.

5 Use Case 1: Event without voice- or multimedia communication

5.1 General

Figure 2 shows the communication model with an alarm sender communicating over the IP network, e.g. Internet, with TS50134 as protocol and an alarm receiver as endpoint. Messages are initiated from either an end user, e.g. human, or a device and could have the function either as an alarm or a status message.

Figure 2 — Communication setup

Figure 3 shows the Alarm Protocol message exchange between the alarm sender and the alarm receiver.

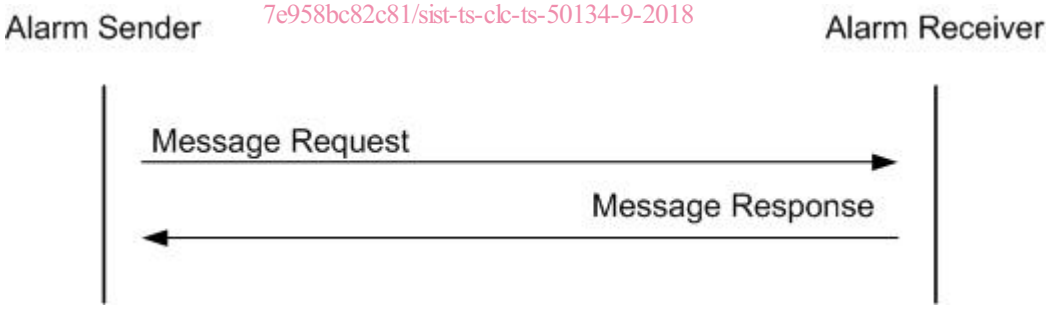

Figure 3 — Message exchange

In this use case, the alarm sender sends a Message Request to the alarm receiver. Each Message Request shall be acknowledged by the alarm receiver using a Message Response.

An event shall be considered successfully handled when the status number (status-number, see Table 2) of the Message Response is set to 0.

5.2 Event not treated by alarm receiver

If the alarm receiver cannot determine the event as treated it shall return a Message Response with status message (status-number, see Table 2) set to 4. This shall cause the alarm sender to resend the same Message Request after 5 to 20 s.

This polling sequence shall continue for at least 3 min but shall not continue for more than 30 min.