IEC 60839-7-4

Edition 1.0 2001-03

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Alarm systems –
Part 7-4: Message formats and protocols for serial data interfaces in alarm transmission systems – Common transport layer protocol

Systèmes d'alarme –
Partie 7-4: Formats de message et protocoles pour les interfaces de données série dans les systèmes de transmission d'alarme – Protocole de la couche commune de transport

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland
Email: inmail@iec.ch
Web: www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

- Catalogue of IEC publications: www.iec.ch/searchpub
The IEC on-line Catalogue enables you to search by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, withdrawn and replaced publications.
- IEC Just Published: www.iec.ch/online_news/justpub
Stay up to date on all new IEC publications. Just Published details twice a month all new publications released. Available on-line and also by email.
- Electropedia: www.electropedia.org
The world's leading online dictionary of electronic and electrical terms containing more than 20 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary online.
- Customer Service Centre: www.iec.ch/webstore/custserv
If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:
Email: csc@iec.ch
Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00

A propos de la CEI

La Commission Electrotechnique Internationale (CEI) est la première organisation mondiale qui élabore et publie des normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications CEI

Le contenu technique des publications de la CEI est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

- Catalogue des publications de la CEI: www.iec.ch/searchpub/cur_fut-f.htm
Le Catalogue en-ligne de la CEI vous permet d'effectuer des recherches en utilisant différents critères (numéro de référence, texte, comité d'études,…). Il donne aussi des informations sur les projets et les publications retirées ou remplacées.
- Just Published CEI: www.iec.ch/online_news/justpub
Restez informé sur les nouvelles publications de la CEI. Just Published détaille deux fois par mois les nouvelles publications parues. Disponible en-ligne et aussi par email.
- Electropedia: www.electropedia.org
Le premier dictionnaire en ligne au monde de termes électroniques et électriques. Il contient plus de 20 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International en ligne.
- Service Clients: www.iec.ch/webstore/custserv/custserv_entry-f.htm
Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions, visitez le FAQ du Service clients ou contactez-nous:
Email: csc@iec.ch
Tél.: +41 22 919 02 11
Fax: +41 22 919 03 00

IEC 60839-7-4

Edition 1.0 2001-03

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Alarm systems –
Part 7-4: Message formats and protocols for serial data interfaces in alarm transmission systems – Common transport layer protocol

Systèmes d'alarme –
Partie 7-4: Formats de message et protocoles pour les interfaces de données série dans les systèmes de transmission d'alarme – Protocole de la couche commune de transport

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

PRICE CODE
CODE PRIX

L

ICS 13.320

ISBN 2-8318-6016-4

SOMMAIRE

CONTENTS

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

SYSTÈMES D'ALARME –

Partie 7-4: Formats de message et protocoles pour les interfaces de données série dans les systèmes de transmission d'alarme – Protocole de la couche commune de transport

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (CEI) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de la CEI). La CEI a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, la CEI – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de la CEI"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec la CEI, participent également aux travaux. La CEI collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de la CEI concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de la CEI intéressés sont représentés dans chaque comité d'études.
3) Les Publications de la CEI se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de la CEI. Tous les efforts raisonnables sont entrepris afin que la CEI s'assure de l'exactitude du contenu technique de ses publications; la CEI ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de la CEI s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de la CEI dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de la CEI et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) La CEI n'a prévu aucune procédure de marquage valant indication d'approbation et n'engage pas sa responsabilité pour les équipements déclarés conformes à une de ses Publications.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à la CEI, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de la CEI, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de la CEI ou de toute autre Publication de la CEI, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de la CEI peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. La CEI ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et de ne pas avoir signalé leur existence.

La Norme internationale CEI 60839-7-4 a été établie par le comité d'études 79 de la CEI: Systèmes d'alarme.

La présente version bilingue, publiée en 2001-11, correspond à la version anglaise.

Le texte anglais de cette norme est basé sur les documents 79/201/FDIS et 79/211/RVD. Le rapport de vote 79/211/RVD donne toute information sur le vote ayant abouti à l'approbation de cette norme.

La version française de cette norme n'a pas été soumise au vote.

Cette publication a été rédigée selon les Directives ISO/CEI, Partie 3.

L'annexe A fait partie intégrante de cette norme.

INTERNATIONAL ELECTROTECHNICAL COMMISSION

ALARM SYSTEMS –

Part 7-4: Message formats and protocols for serial data interfaces in alarm transmission systems – Common transport layer protocol

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.

2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.

3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.

4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.

5) IEC provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with an IEC Publication.

6) All users should ensure that they have the latest edition of this publication.

7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.

8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.

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

International Standard IEC 60839-7-4 has been prepared by IEC technical committee 79: Alarm systems.

This bilingual version, published in 2001-11, corresponds to the English version.

The text of this standard is based on the following documents:

FDIS	Report on voting
79/201/FDIS	79/211/RVD

Full information on the voting for the approval of this standard can be found in the report on voting indicated in the above table.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 3.

Annex A forms an integral part of this standard.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant 2004. A cette date, la publication sera:

- reconduite;
- supprimée;
- remplacée par une édition révisée, ou
- amendée.

La CEI 60839-7-4 constitue une partie d'une série de publications présentées sous le titre général: Systèmes d'alarme – Partie 7: Formats de message et protocoles pour les interfaces de données série dans les systèmes de transmission d'alarme.

CEI 60839-7-1:	Généralités
CEI 60839-7-2:	Protocole de la couche commune d'application
CEI 60839-7-3:	Protocole de la couche commune de liaison de données
CEI 60839-7-4:	Protocole de la couche commune de transport
CEI 60839-7-5:	Interfaces des systèmes d'alarme utilisant une configuration bifilaire conforme à l'ISO/CEI 8482
CEI 60839-7-6:	Interfaces des systèmes d'alarme utilisant la recommandation UIT-T V.24/V.28 pour la signalisation
CEI 60839-7-7:	Interfaces des systèmes d'alarme pour les transmetteurs de systèmes d'alarme enfichables
CEI 60839-7-11:	Protocole série à utiliser par les systèmes numériques de communication utilisant la recommandation UIT-T V.23 pour la signalisation au niveau des interfaces avec le RTPC
CEI 60839-7-12:	Interfaces PTT pour les voies de communication dédiées utilisant la recommandation UIT-T V.23 pour la signalisation
CEI 60839-7-20:	Interfaces d'extrémité utilisant la recommandation UIT-T V.24/V.28 pour la signalisation

The committee has decided that the contents of this publication will remain unchanged until 2004. At this date, the publication will be

- reconfirmed;
- withdrawn;
- replaced by a revised edition, or
- amended.

IEC 60839-7-4 forms one of a series of publications presented under the general title: Alarm systems – Part 7: Message formats and protocols for serial data interfaces in alarm transmission systems.

IEC 60839-7-1: General

IEC 60839-7-2: Common application layer protocol

IEC 60839-7-3: Common data link layer protocol

IEC 60839-7-4: Common transport layer protocol

IEC 60839-7-5: Alarm system interfaces employing a two-wire configuration in accordance with ISO/IEC 8482

IEC 60839-7-6: Alarm system interfaces employing ITU-T Recommendation V.24/V.28 signalling

IEC 60839-7-7: Alarm system interfaces for plug-in alarm system transceivers

IEC 60839-7-11: Serial protocol for use by digital communicator systems using ITU-T Recommendation V.23 signalling at interfaces with the PSTN

IEC 60839-7-12: PTT interfaces for dedicated communications using ITU-T Recommendation V.23 signalling

IEC 60839-7-20: Terminal interfaces employing ITU-T Recommendation V.24/V.28 signalling

SYSTÈMES D'ALARME –

Partie 7-4: Formats de message et protocoles pour les interfaces de données série dans les systèmes de transmission d'alarme – Protocole de la couche commune de transport

1 Domaine d'application

La présente partie de la CEI 60839 spécifie la structure des messages de la couche de transport, les formats et les procédures de transmission à utiliser au niveau des interfaces normalisées dans les systèmes de transmission d'alarme. Il convient que cela soit utilisé pour toutes les interfaces dans lesquelles le matériel provenant d'un fournisseur est destiné à travailler en liaison avec le matériel provenant d'autres fournisseurs, et dans lesquelles l'architecture sous-tendue du système ne donne pas les possibilités nécessaires pour supporter la couche d'application commune.

Cette structure suit les recommandations OSI pour un protocole en couche, pour permettre une souplesse dans le choix et l'utilisation des supports de transmission et des protocoles de niveau inférieur, tout en favorisant le maintien du protocole de la couche commune d'application.

Cette norme s'applique également à la transmission d'alarmes et d'autres messages destinés ou provenant de systèmes d'alarme intrusion, incendie, contrôle d'accès et alarme sociale, ainsi qu'à la transmission d'informations destinées ou provenant d'autres systèmes similaires.

La gestion physique des clés d'authentification requises par cette norme ne fait pas partie de la norme.

2 Références normatives

Les documents de référence suivants sont indispensables pour l'application du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

CEI 60839-7-1, *Systèmes d'alarme – Partie 7-1: Formats de message et protocoles pour les interfaces de données série dans les systèmes de transmission d'alarme – Généralités*

3 Définitions

Dans le cadre de cette partie de la CEI 60839, les définitions de la CEI 60839-7-1 s'appliquent.

4 Abréviations

Les abréviations de la CEI 60839-7-1 s'appliquent.

5 Généralités

La couche de transport est responsable du formatage des messages qui proviennent de la couche d'application sous forme adaptée à la transmission à distance, et de l'adjonction de possibilités non existantes à partir du mécanisme de transport qui est sous-tendu.

Même si une liaison qui utilise ce protocole peut être points-multipoints, ou multipoints-multipoints, la couche de transport décrite ici suppose que ces systèmes comprennent un certain nombre de communications point à point agissant indépendamment.

ALARM SYSTEMS –

Part 7-4: Message formats and protocols for serial data interfaces in alarm transmission systems – Common transport layer protocol

1 Scope

This part of IEC 60839 specifies the transport layer message structure, formats and transmission procedures to be used at standard interfaces in alarm transmission systems. This should be used at all such interfaces where equipment from one supplier is intended to interwork with equipment from other suppliers, and where the underlying system architecture does not provide the necessary facilities to support the common application layer.

The structure follows the OSI recommendations for a layered protocol to allow flexibility in the choice and use of lower level transmission media and protocols, whilst maintaining support for the common application layer protocol.

This standard applies equally to the transmission of alarms and other messages to/from intrusion, fire, access control and social alarm systems, and to the transmission of information to/from other similar systems.

The physical management of the authentication keys required by this standard is not included.

2 Normative references

The following referenced documents are indispensable for the application 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.

IEC 60839-7-1, *Alarm systems – Part 7-1: Message formats and protocols for serial data interfaces in alarm transmission systems – General*

3 Definitions

For the purpose of this part of IEC 60839, the definitions in IEC 60839-7-1 apply.

4 Abbreviations

The abbreviations in IEC 60839-7-1 apply.

5 General

The transport layer is responsible for the formatting of messages from the application layer into a form suitable for transmission to the remote location, and for the addition of facilities not available from the underlying transport mechanism.

Although a link using this protocol may be point-multipoint, or multipoint-multipoint, the transport layer described here presumes that such systems will comprise a number of logical point-point communications which will proceed independently.

Dans ces types de communication, un dispositif est défini comme étant l'ORIGINE (ORIGINATOR) et un dispositif comme étant le RÉCEPTEUR (RECEIVER), afin que la norme puisse être définie de manière générale. La norme appelante doit identifier laquelle de ces fonctions est affectée et auquel de ces matériels.

6 Format du message de la couche de transport

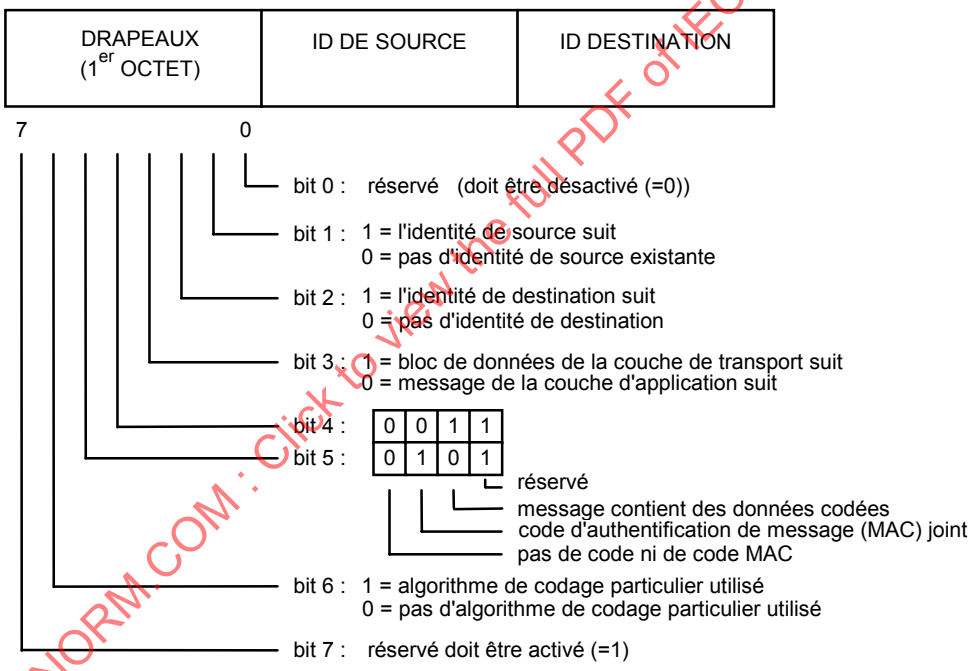
Chaque message de la couche d'application ou chaque bloc de données de la couche de transport doit être formaté dans le message de la couche de transport avec adjonction d'un en-tête tel que celui défini ci-dessous.

6.1 Transmission de blocs de données de la couche de transport

Les données de la couche de transport doivent être formatées conformément à l'annexe A et doivent être transmises avec un en-tête de couche de transport, comme cela est défini en 6.2.

6.2 En-tête de la couche de transport

L'en-tête de la couche de transport doit être le suivant:



Il convient que le bit 4 soit indiqué si le message d'application ou si les données de transport sont codées. Il convient que le bit 5 soit indiqué pour préciser que le message contient un code d'authentification de message (MAC). Il convient de ne pas utiliser l'option d'un codage ni d'un code MAC, car ceci diminue effectivement la sécurité. Si un algorithme de sécurité élevée particulier est utilisé pour un chiffrement ou pour un code MAC, il convient que le bit 6 soit précisé, sinon il convient d'utiliser l'algorithme normalisé défini dans cette norme.

Le bit 3 indique si les données forment un bloc de données de couche de transport ou un message de couche d'application.

L'en-tête de la couche de transport peut inclure l'identité de la source, l'identité de la destination, les deux ou ni l'une ni l'autre comme cela est défini dans les bits 1 et 2.

La longueur maximale pour l'IDENTITÉ DE LA SOURCE (SOURCE ID) et de l'IDENTITÉ DE LA DESTINATION (DESTINATION ID) est de huit octets correspondant chacun à sept chiffres.

Si les deux identités existent, l'identité de la source doit être indiquée en premier lieu.

In such communications, one device is defined as the ORIGINATOR and one as the RECEIVER in order that the standard may be defined generally. The calling standard shall identify which of these functions is assigned to which equipment.

6 Transport layer message format

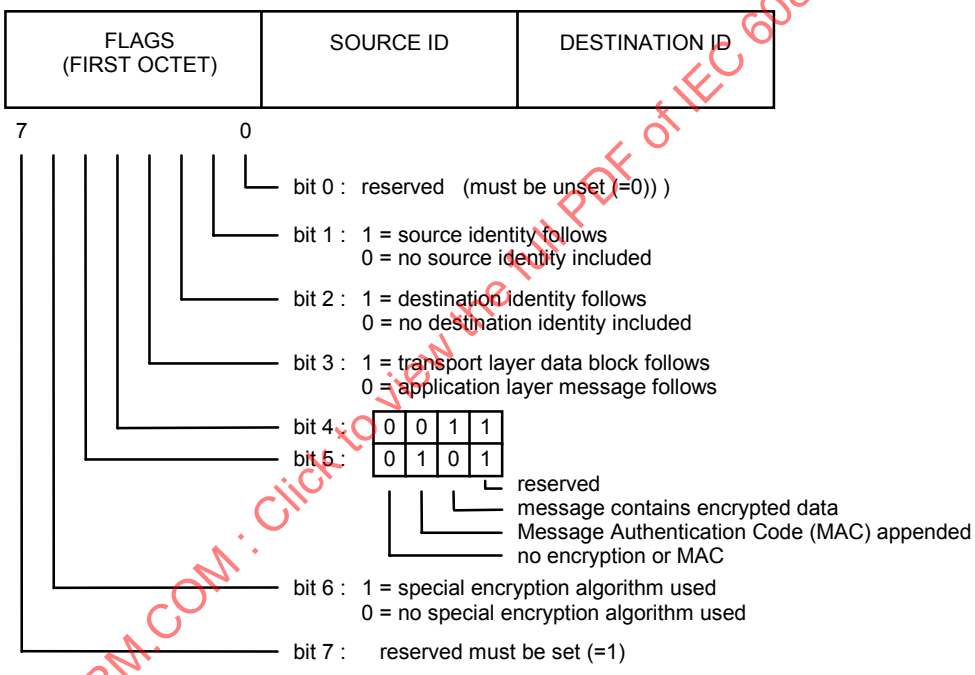
Each application layer message or transport layer data block shall be formatted into transport layer message with the addition of a header as defined below.

6.1 Transmission of transport layer data block

Transport layer data shall be formatted in accordance with annex A and transmitted with a transport layer header as defined in 6.2.

6.2 Transport layer header

The transport layer header shall be as follows:



Bit 4 should be set when the application message or the transport data are encrypted. Bit 5 should be set to indicate that the message contains a message authentication code (MAC). The option of using encryption and a MAC should not be used since this effectively lowers the security. Where a special high security algorithm is used for either the encryption or the MAC bit 6 should be set, otherwise the standard algorithm defined in this standard should be used.

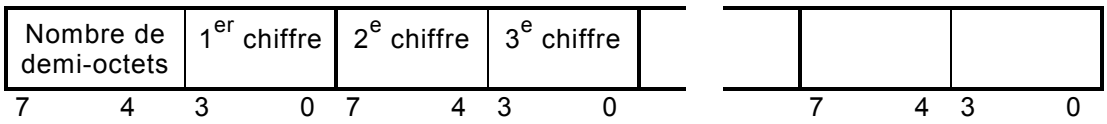
Bit 3 indicates whether the data is a transport layer data block or an application layer message.

The transport layer header may include the source identity, the destination identity, both or neither as defined in bits 1 and 2.

Maximum length for SOURCE ID and DESTINATION ID is eight octets equal to seven digits each.

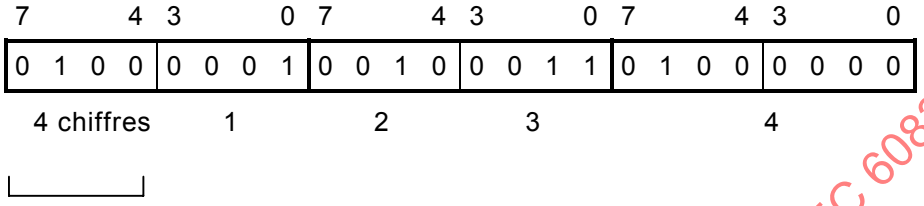
Where both identities are included, the source identity shall always be first.

Le format de l'identité est le suivant:



Le premier demi-octet (bits 4 à 7 du premier octet) est le nombre de chiffres dans l'adresse. Les chiffres de l'identité réelle doivent être contenus dans les demi-octets correspondant, en format hexadécimal, en commençant par le demi-octet le plus faible du premier octet. L'identité doit seulement contenir un nombre suffisant d'octets pour inclure le nombre de chiffres requis. Si le nombre de chiffres est pair, le dernier demi-octet (bits 0 à 3 du dernier octet) doit être zéro.

Par exemple si l'identité est 1234, il convient que ceci soit transmis comme indiqué ci-après:



7 Authentification

La procédure suivante doit être adoptée, après avoir établi la connexion, pour confirmer l'identité du matériel.

7.1 Configuration

Comme partie constitutive de son initialisation/sa configuration, chaque morceau de matériel doit être programmé avec une clé maître (Mk).

7.2 Initialisation

Une liaison étant établie, l'ORIGINE (ORIGINATOR) doit générer deux nombres aléatoires R1 et Rs, et doit transmettre au RÉCEPTEUR (RECEIVER) R1, message codé de type 1 avec la clé Mk, en tant que message de couche de transport (voir annexe A). Rs est le tirage aléatoire utilisé par l'algorithme de codage pour la transmission de R1.

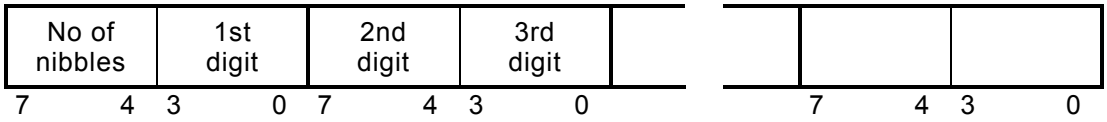
Le RÉCEPTEUR (RECEIVER) doit décoder R1 et doit alors générer un nombre aléatoire R2 en même temps qu'une clé secondaire Ki. Il doit alors retourner un message de type 2, message de couche de transport, à l'ORIGINE (ORIGINATOR) contenant R2 en même temps que R1 et Ki. Ce message doit être codé en utilisant Mk et Ki comme cela est indiqué ci-dessous et dans l'annexe A.

La valeur de la clé secondaire (Ki) et les nombres aléatoires R1 et R2 doivent uniquement être stockés dans la mémoire volatile, et il convient qu'il ne soit pas possible de l'afficher ni dans le RÉCEPTEUR (RECEIVER) ni dans l'ORIGINE (ORIGINATOR).

L'ORIGINE (ORIGINATOR) doit décoder le message pour évaluer R1, R2 et Ki. La réception correcte de R1 confirme l'identité du RÉCEPTEUR (RECEIVER). Si elle est correcte, il doit alors envoyer un message de type 3 de la couche de transport, message contenant R2 codé en utilisant Ki. Le décodage correct de R2 au niveau du RÉCEPTEUR (RECEIVER) confirme l'identité de l'ORIGINE (ORIGINATOR).

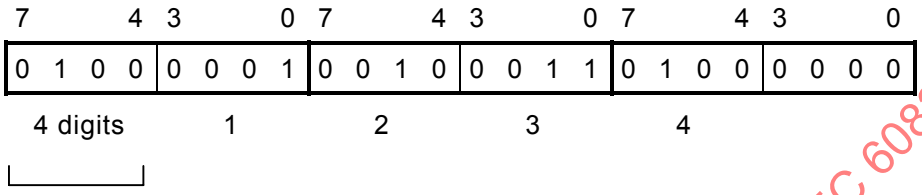
Un message doit être généré à la fois vers le système d'alarme et le matériel d'affichage pour indiquer que cette valeur de Ki a été activée.

The format of the identity is as follows:



The first nibble (bits 4-7 of the first octet) is the number of digits in the address. The actual identity digits shall be contained in subsequent nibbles in HEX format, starting with the lower nibble of the first octet. The identity shall contain only sufficient octets to include the number of digits required. If the number of digits is even, the last nibble (bits 0-3 of the last octet) shall be zero.

As an example, if the identity is 1234 this would be transmitted as:



7 Authentication

The following procedure shall be adopted following the establishment of the connection in order to confirm the identity of the equipment.

7.1 Configuration

As part of their initialization/configuration each item of equipment shall be programmed with a master key (Mk).

7.2 Initialization

With a connection established, the ORIGINATOR shall generate two random numbers R1 and Rs, and shall transmit R1 to the RECEIVER encrypted with Mk as transport layer message type 1 (see annex A). Rs is the random seed used by the encryption algorithm for the transmission of R1.

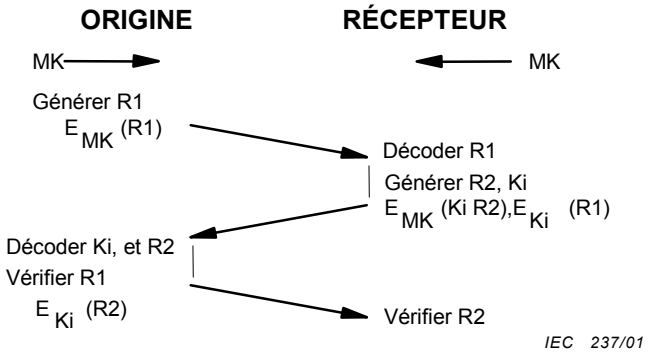
The RECEIVER shall decode R1 and shall then generate a random number R2, together with a secondary key Ki. It shall then return a transport layer message type 2 to the ORIGINATOR which contains R2 together with R1 and Ki. This message shall be encrypted using Mk and Ki as shown below and in annex A.

The value of the secondary key (Ki) and the random numbers R1 and R2 shall only be stored in volatile memory and should not be capable of being displayed in either the RECEIVER or ORIGINATOR.

The ORIGINATOR shall decode the message to evaluate R1, R2 and Ki. The correct reception of R1 confirms the identity of the RECEIVER. If correct, it shall then send a transport layer message type 3 containing R2 encrypted using Ki. The correct decoding of R2 at the RECEIVER confirms the identity of the ORIGINATOR.

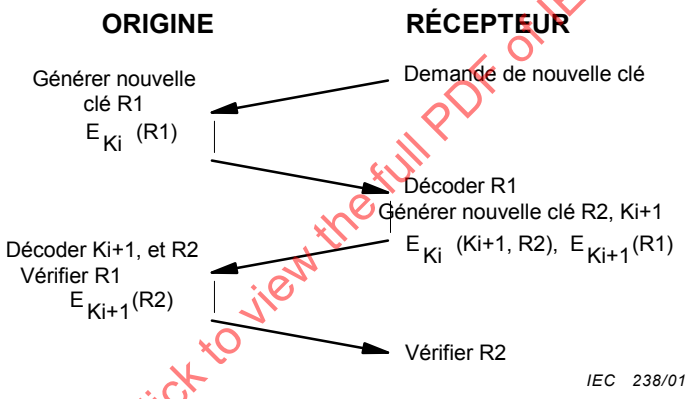
A message shall be generated to both the alarm system and the annunciation equipment to indicate that the value of Ki has been set.

Toutes les communications qui en découlent doivent être codées en utilisant la clé secondaire Ki à la fois pour la connexion en cours et pour toutes les connexions qui en découlent jusqu'à ce que la valeur de Ki soit modifiée.



7.3 Modification de la clé secondaire

Le RÉCEPTEUR (RECEIVER) doit périodiquement initier une modification de la valeur de Ki en transmettant un message de type 4 de couche de transport. Ceci doit uniquement être réalisé après avoir établi une connexion et ceci doit être réalisé comme suit:



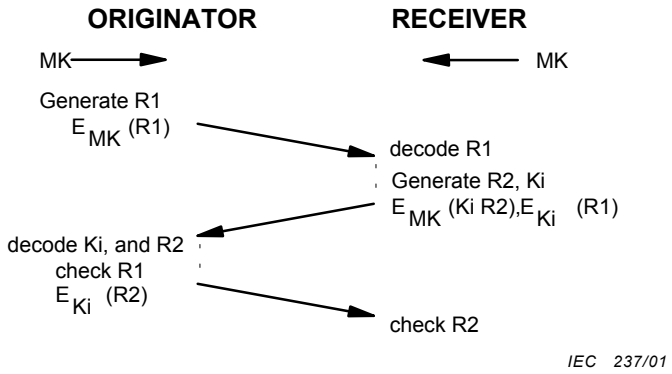
La nouvelle valeur de la clé (Ki+1) doit être utilisée pour la transmission et la réception de tous les messages par l'ORIGINE (ORIGINATOR) après avoir transmis le dernier message défini ci-dessus, et par le RÉCEPTEUR (RECEIVER) après avoir reçu le message.

7.4 Défaillance de synchronisation

Si la communication est établie en clair, mais que les données ne peuvent pas être échangées sous forme codée, alors la séquence d'initialisation définie ci-dessus doit être répétée. Si la communication codée n'est pas possible au deuxième essai, un message d'alarme ou de défaillance doit être généré vers le système d'alarme et le matériel d'affichage, et, en outre, la communication doit cesser.

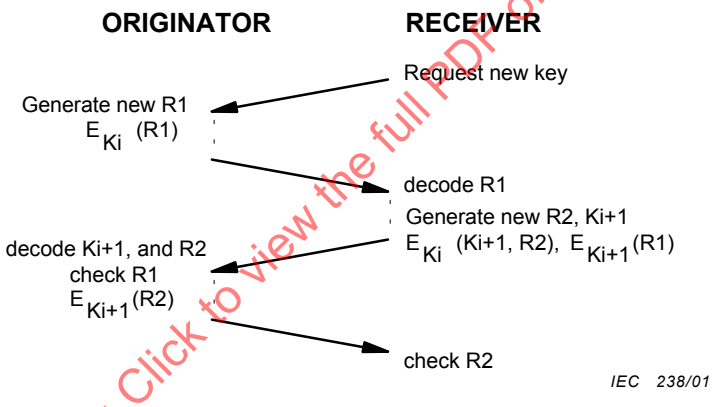
Si les communications codées ne sont pas possibles, un essai peut être fait pour synchroniser de nouveau les communications en initialisant de nouveau les clés par utilisation de Mk. Quand ceci a été effectué, un message d'alarme ou de défaillance doit être généré vers le système d'alarme et le matériel d'affichage pour indiquer que cette valeur de Ki a été activée de nouveau. Pour une application dans laquelle la sécurité est importante, il convient uniquement de faire ceci après une intervention manuelle ou quand le matériel est dans un mode particulier (par exemple essai d'ingénierie).

All subsequent communication shall be encrypted using the secondary key Ki both for the current connection and for all subsequent connections until the value of Ki is changed.



7.3 Change of secondary key

The RECEIVER shall periodically initiate a change of the value of Ki by transmitting a transport layer message type 4. This shall only be done after a connection has been established and shall be carried out as follows:



The new value of key (Ki+1) shall be used for the transmission and reception of all messages by the ORIGINATOR after it has transmitted the last message defined above, and by the RECEIVER after it has received the message.

7.4 Failure of synchronization

If communication is established in plain text but data cannot be exchanged in an encrypted form, then the initialization sequence defined above shall be repeated. If the encrypted communication fails on the second attempt an alarm or fault message shall be generated to both the alarm system and the annunciation equipment and further communication shall cease.

If encrypted communications fail an attempt may be made to re-synchronize the communications by re-initializing the keys using Mk. Where this is done, an alarm or fault message shall be generated to both the alarm system and the annunciation equipment to indicate that the value of Ki has been reset. For application where security is important, this should only be done following manual intervention or when the equipment is in a special mode (e.g. engineering test).

7.5 Longueur des clés

Tous les nombres et toutes les clés aléatoires indiqués ci-dessus doivent être choisis à partir d'un octet de huit bits dont toutes les valeurs ont vraisemblablement la même probabilité d'exister, excepté que les valeurs hexadécimales 00 HEX et FF HEX ne doivent pas être utilisées. La valeur de Ki doit être unique pour chaque ORIGINE (ORIGINATOR).

8 Codage

Si un codage est demandé pour des images contenant un message d'application, ce codage doit être fourni sur tous les octets qui suivent l'en-tête de la couche de transport. Le bit 4 du premier octet d'en-tête de la couche de transport doit être activé (=1).

Si un codage est requis dans les messages de la couche de transport, ce codage doit être fourni en groupes d'octets comme défini dans l'annexe A. Le bit 4 du premier octet d'en-tête de la couche de transport doit être activé (=1).

Pour certaines applications de très haute sécurité utilisant ce protocole, l'algorithme de codage normalisé décrit ci-dessous peut ne pas être considéré comme adéquat. Dans ces cas, il convient que le bit 6 du premier octet d'en-tête de la couche soit activé (=1) pour indiquer l'utilisation d'un algorithme différent.

9 Code d'authentification des messages (MAC)

Si un code MAC est requis dans les messages contenant un message d'application, il doit être fourni sur tous les octets qui suivent l'en-tête de la couche de transport. Le code MAC doit être inclus en fin de message sous forme d'un octet unique. Le bit 5 du premier octet d'en-tête de la couche de transport doit être activé (=1).

Pour les messages dotés d'un code MAC, le premier octet du message transmis sera le TIRAGE ALÉATOIRE (RANDOM SEED). Ceci sera suivi par les octets sources (SOURCE 1 – SOURCE N) et puis le résultat (RESULT) N+1. Les messages dotés d'un code MAC seront plus longs de deux octets que le message du texte en clair équivalent.

7.5 Size of keys

All of the above random numbers and keys shall be chosen from an eight bit octet with all values equally likely, except that the values 00 HEX and FF HEX shall not be used. The value of Ki shall be unique for each ORIGINATOR.

8 Encryption

Where encryption is required in images containing an application message, it shall be provided on all octets following the transport layer header. Bit 4 in the first octet of the transport layer header shall be set (=1).

Where encryption is required in transport layer messages, it shall be provided on groups of octet as defined in annex A. Bit 4 in the first octet of the transport layer header shall be set (=1).

For some very high security applications using this protocol, it may be that the standard encryption algorithm described below is not considered adequate. In such cases, bit 6 in the first octet of the transport layer header should be set (=1) to indicate the use of a different algorithm.

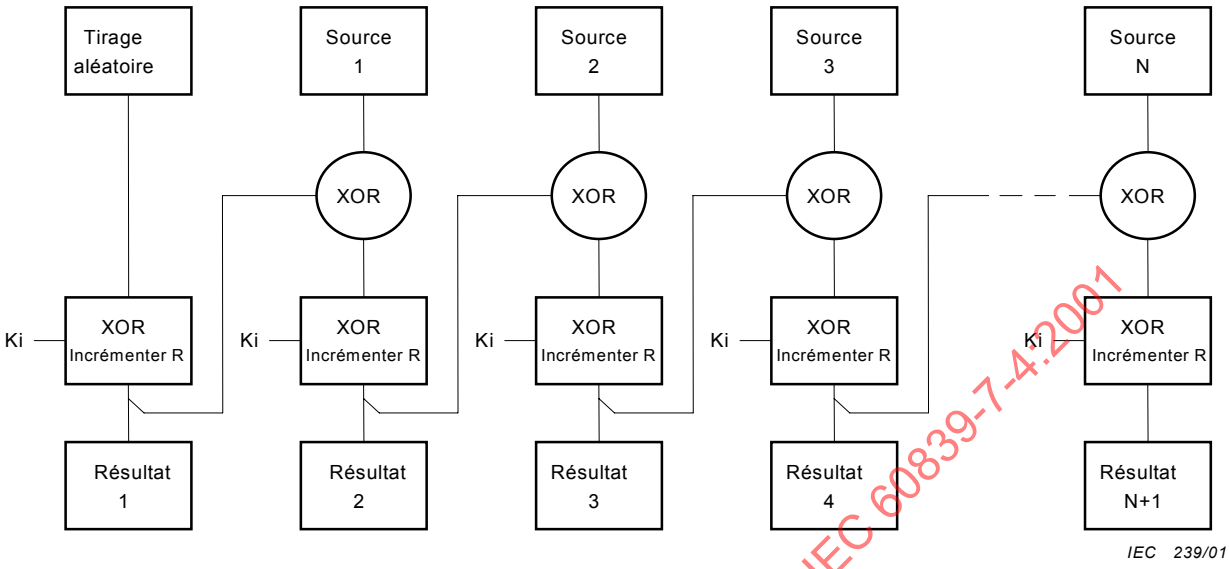
9 Message authentication code (MAC)

Where a MAC is required in messages containing an application message, it shall be provided on all octets following the transport layer header. The MAC shall be included at the end of the message as a single octet. Bit 5 in the first octet of the transport layer header shall be set (=1).

For messages with a MAC, the first octet of the transmitted message will be the RANDOM SEED. This will be followed by the source octets (SOURCE 1 – SOURCE N) and then RESULT N+1. Messages with a MAC will be two octets longer than the equivalent plain text message.

10 Algorithme normalisé

L'algorithme de codage de bloc suivant doit être utilisé pour le codage ou le codage MAC:



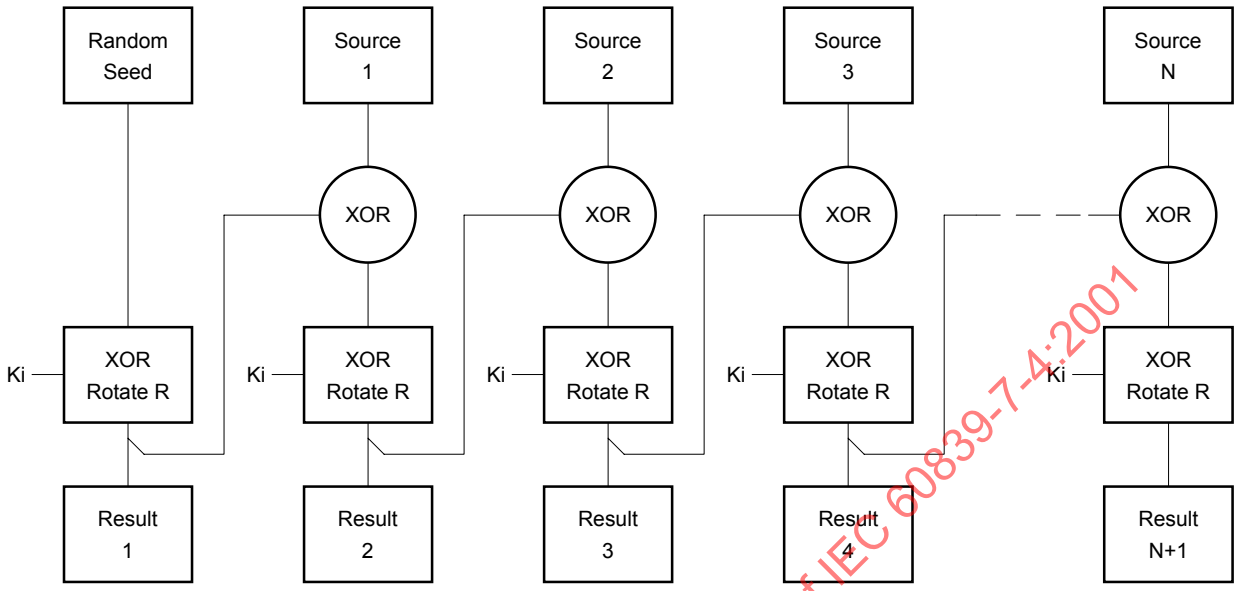
Le tirage aléatoire utilisé pour tous les messages d'authentification doit être celui défini en annexe A. Pour les messages qui en découlent, ce peut être un nombre aléatoire quelconque.

NOTE Pour une meilleure sécurité, il convient que le nombre aléatoire soit le dernier octet du dernier message transmis. Le matériel de réception peut alors le déchiffrer et le comparer à la valeur correspondante provenant du dernier message reçu. Alors que ceci n'évite pas la substitution des messages provenant de quelqu'un qui connaît la clé et l'algorithme en cours, ceci permet de détecter la substitution si un message authentique est reçu après.

Pour les messages codés, le message transmis sera constitué des octets RÉSULTAT (RESULT) 1 – RÉSULTAT (RESULT) N+1. Les messages codés seront plus longs d'un octet que le message du texte clair équivalent.

10 Standard algorithm

The following block encryption algorithm shall be used for either encryption or MAC:



The random seed used for all authentication messages shall be as defined in annex A. For all subsequent messages it may be any random number.

NOTE For increased security, the random number should be the last octet of the last message transmitted. The receiving equipment can thus decrypt it and compare with the corresponding value from the last message received. Whilst this does not prevent message substitution from someone who knows the both current key and the algorithm, it enables substitution to be detected when a genuine message is next received.

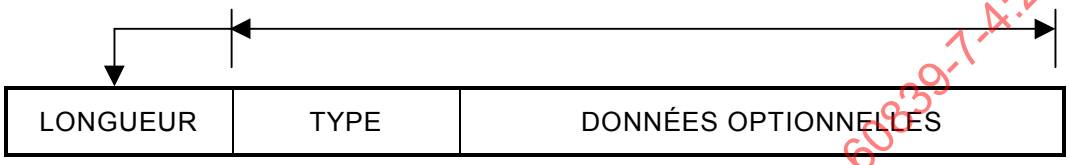
For encrypted messages the transmitted message will be the octets RESULT 1 – RESULT N+1. Encrypted messages will be one octet longer than the equivalent plain text message.

Annexe A
(normative)

Messages de la couche de transport

Sauf si cela est indiqué, tous les nombres se référant à cette annexe sont dans le format hexadécimal. Les types de message non utilisés ci-dessous A0 HEX sont réservés à des utilisations futures. Les types au-delà de A0 HEX sont disponibles pour des extensions particulières destinées au fabricant.

Le bloc de données de la couche de transport doit comprendre deux octets, ou plus comme cela est indiqué:



IEC 240/01

Le premier octet doit toujours être la longueur et doit être le nombre d'octets dans le bloc de données de la couche transport qui suit l'octet indiquant la longueur.

Le second octet du bloc de données de la couche transport doit toujours être le type de message d'authentification, comme cela est défini dans les articles qui suivent.

Un ou plusieurs octets de données peuvent être ajoutés comme message de la couche de transport, comme cela est indiqué ci-dessous. Le nombre d'octets de données ne doit pas dépasser 235 octets, mais il faut noter que si un certain nombre de blocs de données de la couche de transport sont constitués en un message unique de couche de transport, la longueur maximale de ces blocs de données de couche de transport ne doit pas dépasser 237 octets.

A.1 Messages de la couche de transport

Les messages suivants de la couche de transport sont définis dans leur format non codé. Pour ceux dont le codage est obligatoire, le diagramme associé décrit la manière de déduire le bloc de messages transmis.

A.1.1 Message d'authentification de type 1

Référence à l'article 10, algorithme normalisé

Longueur de la source 1	:	2
Type de la source 2	:	1
Octet 1 de données de la source 3	:	R1
Format transmis	:	codé
Tirage aléatoire	:	Rs
Clé de codage	:	Ki

Pour la première authentification, il convient que la procédure Rs soit générée par l'ORIGINE (ORIGINE) et que la clé de codage (Ki) soit Mk.

Pour la mise à jour des clés suivantes, il convient que Rs soit le dernier octet transmis du dernier message transmis (soit le message de la couche transport, soit le message de la couche d'application).