(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 813 130**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **01 10641**

(51) Int Cl[7] : **G 05 B 19/048,** H 04 L 12/28

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 09.08.01.

(30) **Priorité :** 09.08.00 DE 10038779.

(43) **Date de mise à la disposition du public de la demande :** 22.02.02 Bulletin 02/08.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Ce dernier n'a pas été établi à la date de publication de la demande.*

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *SCHNEIDER AUTOMATION GMBH Gesellschaft mit beschränkter Haftung* — DE.

(72) **Inventeur(s) :** SUSSMANN BORIS.

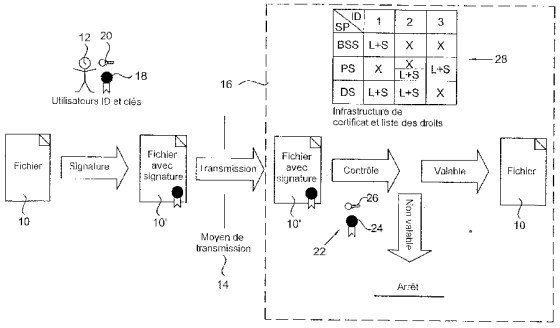
(73) **Titulaire(s) :**

(74) **Mandataire(s) :** CABINET HERRBURGER.

(54) PROCEDE D'ECHANGE DE DONNEES AVEC APPAREIL DE COMMANDE TEL QU'UNE COMMANDE A MEMOIRE PROGRAMMABLE ET APPAREIL DE COMMANDE AINSI EQUIPE.

(57) Procédé utilisant un appareil de commande (16) effectuant, les étapes suivantes:

- codage de données (10) à l'émission avec au moins une caractéristique (18, 24) et à la réception et contrôle de la caractéristique (18, 24),
- comparaison de la caractéristique (18, 24) avec des caractéristiques définies (ID 1, ID 2... ID n),
- attribution de droits d'utilisation pour des modifications selon une liste d'autorisations (28) enregistrée du côté de la réception,
- rejet des données (10) si la caractéristique d'émetteur (18) individuelle n'est pas valable.



FR 2 813 130 - A1

La présente invention concerne un procédé d'échange de données avec un appareil de commande et un appareil de commande ainsi réalisé.

Selon l'état de la technique, les mises à jour de programmes d'un appareil de commande comme par exemple les mises à jour des programmes d'applications sont effectuées par un technicien avec un appareil de programmation particulier qui effectue les opérations sur place. Après introduction du mot de passe, le technicien accède à l'ensemble de la zone de mémoire, ce qui lui permet d'intervenir. Mais souvent, il est nécessaire de permettre à l'utilisateur de l'appareil de commande d'avoir des accès correspondants par exemple pour modifier et actualiser des données du procédé. Mais l'inconvénient sera que du personnel non qualifié risque de détruire des parties importantes du programme.

Depuis peu, on peut manipuler ou programmer des appareils de commande telles que des commandes programmées par programmation en mémoire également par des réseaux d'échange de données comme par exemple un réseau Intranet ou le réseau Internet. Mais on risque alors que des personnes non autorisées et/ou des programmes/données non autorisés, puissent être accédés dans les commandes à programmes en mémoire et produire ainsi des modifications d'état non voulues des commandes avec programmes inscrits en mémoire.

A partir de cette situation, la présente invention a pour but de développer un procédé et un appareil de commande correspondant au type défini ci-dessus pour améliorer la sécurité de l'échange des données avec l'appareil de commande. En particulier, seules les personnes autorisées doivent pouvoir accéder à l'appareil de commande.

A cet effet, l'invention concerne un procédé du type défini ci-dessus caractérisé par les étapes suivantes :

- codage de données du côté de l'émission avec au moins une caractéristique d'émetteur individuelle,
- décodage des données du côté de la réception et contrôle de la caractéristique individuelle d'émetteur pour en vérifier la validité,
- comparaison de la caractéristique individuelle d'émetteur avec des caractéristiques d'émetteur définies,
- attribution de droits d'utilisation pour des modifications d'état des données transmises et/ou de l'appareil de commande selon une liste d'autorisations enregistrée du côté de la réception dans la mesure où la caractéristique d'émetteur individuelle est contenue dans la liste

d'autorisations et, rejet des données dans la mesure où la caractéristique d'émetteur individuelle n'est pas valable ou n'est pas contenue dans la liste d'autorisations.

Le procédé selon l'invention offre l'avantage de ne permettre qu'à des personnes autorisées avec des caractéristiques d'émetteur, définies et/ou des programmes codés de manière correspondante, d'accéder à l'appareil de commande. Cela garantit qu'une modification des programmes et des applications ainsi que des données de procédé contenues dans la mémoire de l'appareil de commande ne puissent être faites que par le fabricant ou des personnes qu'il autorise.

Un mode de réalisation préférentiel prévoit de coder les données du côté de l'émetteur avec une signature numérique et/ou une clé publique, et de décoder les données du côté de la réception avec une clé secrète correspondante et/ou de vérifier la signature numérique. Cela signifie que pour chaque transfert de données échangées avec un appareil de commande tel qu'une commande à programmes en mémoire (SPS), il y a une signature numérique. Après un transfert, on vérifie tout d'abord la signature. Si celle-ci n'est pas valable, les données transférées sont rejetées ; dans le cas contraire, on vérifie si le signataire est autorisé pour exécuter le transfert. Dans la mesure où l'émetteur possède les droits, les données seront traitées ; au cas contraire, les données transférées seront rejetées.

Si un utilisateur signe numériquement les données, il ajoute sa signature numérique aux données et le cas échéant un certificat. Un certificat se compose comme cela est habituel dans le domaine des signatures numériques, d'au moins une caractéristique ainsi que de la clé officielle du titulaire du certificat et la signature numérique de l'émetteur du certificat par les données du titulaire. Dans l'appareil de commande, on peut utiliser l'identité et l'autorisation de l'émetteur ou du signataire pour vérifier la signature numérique et la clé officielle correspondante pour répondre avec des données codées que seul l'émetteur d'origine peut lire avec sa clé privée. Il est également possible de coder les données du côté de l'émission avec la clé publique d'un récepteur et d'un appareil de commande.

Si l'appareil de commande ne peut vérifier directement le certificat, l'infrastructure des certificats lui envoie, des certificats jusqu'à ce que soit établie une chaîne de certificats qui peut être vérifiée sans faille par un certificat vérifiable.

Dans la transmission des données d'un appareil vers un récepteur, il est prévu de coder les données dans l'appareil de commande avec une signature numérique pour éviter toute manipulation ultérieure des données.

En particulier, on peut définir les types de transmissions et/ou les plages limites et pour une transmission de données à partir de l'appareil de commande, on effectue un codage avec une signature numérique et/ou une clé publique et/ou une clé privée.

De manière préférentielle, la liste d'autorisations est enregistrée du côté de la réception dans une mémoire de l'appareil de commande. La zone de mémoire elle-même se commande de manière précise par le codage du fichier à transmettre. La liste d'autorisations est également adaptable individuellement.

Pour augmenter encore plus la sécurité, il est prévu d'attribuer également des droits d'accès pour les listes d'autorisations enregistrées dans l'appareil de commande. En d'autres termes, une personne non autorisée ne peut violer la protection en manipulant les listes autorisées.

Un appareil de commande ainsi qu'une commande programmable par un programme en mémoire se caractérise en ce qu'ils comportent une unité de réception avec une unité de décodage pour décoder au moins une caractéristique d'émetteur dans les données reçues ; l'appareil de commande possède une liste d'autorisations dans lequel les différentes caractéristiques d'émetteur reçoivent des droits de changement d'état de l'appareil de commande. L'état de l'appareil de commande en cas de reconnaissance d'émetteur, valable et inscrite dans la liste d'autorisations, permet de modifier les droits donnés dans la liste.

Pour assurer que les données envoyées par l'appareil de commande réalisé comme une commande à programme en mémoire, ne risquent pas d'être manipulées ultérieurement, il est prévu que l'appareil de commande comporte une unité d'émetteur avec une installation de codage pour coder les données à émettre et l'installation de codage contient une signature numérique et/ou une clé publique pour le codage des données.

La zone de mémoire de l'appareil de commande est subdivisée en zones définies et à chaque zone de mémoire dans la liste d'autorisations sont définis des droits pour différentes reconnaissances d'émetteur. Par exemple, le fabricant peut attribuer des droits selon les-

quels une zone de mémoire de programme ne peut être manipulée qu'avec la caractéristique d'émetteur attribuée par le fabricant. Il en résulte l'avantage que les programmes puissent être actualisés par Internet et également être fournis sous la forme d'un fichier que le client de la commande à programme en mémoire enregistre lui-même. Comme la signature du fichier perd sa validité en cas de manipulations, seule l'actualisation autorisée peut s'enregistrer.

La construction de la commande à programme en mémoire selon l'invention, offre en outre l'avantage que le fabricant de la machine (appelé dans ce cas OEM) qui utilise la commande à programme en mémoire pour commander une installation de production, peut définir l'autorisation pour une mémoire à programme utilisée par le fabricant OEM, de façon que seul ce fabricant OEM puisse inscrire dans cette zone et qu'aucune personne non autorisée puisse lire cette zone. La liste d'autorisations peut être réglée pour qu'un client du fabricant OEM puisse enregistrer d'autres parties de programme dans les zones de mémoire non protégées.

Pour protéger encore plus la transmission des données, il est prévu un transfert des données codées. Cela permet par exemple de transmettre des données de procédé de la commande à programme en mémoire également par des moyens non protégés comme par exemple Internet. Un transfert de données codées peut également être utilisé par un fabricant OEM pour lire un programme d'application dans la commande à programme en mémoire sans que ce programme d'application ne puisse être décodé par des tiers au moment de son transfert.

La présente invention sera décrite ci-après de manière plus détaillée à l'aide d'un mode de réalisation représenté dans l'unique figure annexée qui montre de manière purement schématique un procédé de transmission.

L'unique figure montre un procédé de transmission d'un fichier 10 par un émetteur tel qu'une personne autorisée 12 par l'intermédiaire d'un moyen 14 qui, dans le cas présent, est un réseau de transmission de données comme un réseau Intranet ou Internet, vers un récepteur 16 qui, dans le présent exemple de réalisation est un appareil de commande 16 tel qu'une commande à programme en mémoire ou une commande utilisant un PC.

Le fichier 10 à envoyer est tout d'abord codé ; pour cela, on ajoute au fichier 10, une signature numérique 18 de l'utilisateur 12 et une

clé publique 20. La combinaison de la signature numérique 18 et de la clé publique 20 peut également s'appeler certificat fourni par une autorité de certification (CA) comme par exemple le Veri Sign. De cette manière, le fichier 10' codé ou signé est transmis à l'état codé par le moyen 14. La commande à programme en mémoire 16 contient un certificat de base 22 comprenant une signature numérique 24 ainsi qu'une clé secrète privée et/ou publique 20 pour décoder le fichier 10'. Si la signature 18 n'est pas valable, le fichier transféré 10' sera rejeté. Si la signature 18 est valable, on vérifie si l'utilisateur 12 est autorisé à effectuer le transfert. Pour cela, l'appareil de commande 16 contient une liste d'autorisations 28 sous la forme d'un tableau. Si les droits existent, on peut traiter le fichier 10. Dans la zone de mémoire de la commande 16 à mémoire en programme, selon un exemple de réalisation, la mémoire est subdivisée en zones définies (BSS, PS, DS). Pour chaque zone de mémoire comme par exemple la mémoire du système de fonctionnement (BSS), la mémoire de programme (PS ainsi que la mémoire de données (DS), on a dans les tableaux 28 pour chaque reconnaissance d'émetteur ID 1, ID 2 ... IDn, c'est-à-dire chaque signature numérique du côté de l'émetteur ID 1, ID 2 ... IDn, on a défini des droits comme par exemple lecture (L) et/ou enregistrement (S).

Dans l'exemple de réalisation représenté, le tableau 28 définit globalement trois utilisateurs ID 1 ... ID 3 ainsi que trois zones de mémoire BSS, PS et DS. Un fabricant de la commande à programme en mémoire 16 est par exemple affecté de la caractéristique d'émetteur ID 1. Dès qu'un fichier 10' est reconnu avec la signature ID 1, les droits de lecture et d'écriture pour toutes les zones de mémoire sont attribués. Par le tableau d'autorisations tel que représenté, par exemple seul le fabricant est autorisé à intervenir dans la zone de mémoire de programme BSS. On peut également fournir par exemple un fichier signé 10' à un client avec la possibilité pour le client d'introduire le fichier dans la commande à programme en mémoire 16 sans accéder à la mémoire elle-même.

Il est également possible pour un fabricant de machines (OEM), de programmer l'autorisation qui lui est attribuée pour la mémoire de programme, pour que seul le fabricant OEM puisse inscrire dans cette zone et qu'une personne non autorisée ne puisse pas lire ; toutefois le client doit pouvoir introduire d'autres parties de programme dans des zones de mémoire de programme, non protégées.

Il est également possible que la commande à programme en mémoire 16 contienne elle-même une infrastructure de certificat formée

de la clé publique 26, d'une clé privée et d'une signature numérique 24. Cela permet de définir des types de transfert ou des zones de mémoire pour lesquels la commande à programme en mémoire signe numériquement les données, ce qui interdit toute manipulation ultérieure des données. Il est évident que pour le tableau 28/liste d'autorisations, on utilise des droits d'accès pour qu'une personne non autorisée ne puisse violer la protection en manipulant les listes.

De plus, l'infrastructure de certificat 18, 20, 22, 24, 26 permet également d'assurer un transfert de données codées pour que les données du procédé puissent également se transmettre à partir de la commande à programme en mémoire par des moyens comme par exemple le réseau Internet. Le transfert codé des données peut également être utilisé par un fabricant de machines (OEM) pour lire des programmes d'application dans l'appareil sans que des tiers ne puissent y accéder.

TRADUCTION DE LA FIGURE

10 fichier
100 utilisateurs ID et clés
101 signature
10' fichier avec signature
102 transmission
14 moyens de transmission
10' fichier avec signature
104 infrastructure de certificat et liste des droits
105 contrôle
106 valable
107 non valable
108 arrêt
10 fichier

REVENDICATIONS

1°) Procédé d'échange de données avec un appareil de commande (16) tel qu'une commande à programme en mémoire,
caractérisé par les étapes suivantes :

- codage de données (10) du côté de l'émission avec au moins une caractéristique d'émetteur (18, 24) individuelle,
- décodage des données (10) du côté de la réception et contrôle de la caractéristique individuelle d'émetteur (18, 24) pour en vérifier la validité,
- comparaison de la caractéristique individuelle d'émetteur (18, 24) avec des caractéristiques d'émetteur définies (ID 1, ID 2 ... ID n),
- attribution de droits d'utilisation pour des modifications d'état des données transmises (10) et/ou de l'appareil de commande selon une liste d'autorisations (28) enregistrée du côté de la réception dans la mesure où la caractéristique d'émetteur individuelle (18, 24) est contenue dans la liste d'autorisations (28) et,
- rejet des données (10) dans la mesure où la caractéristique d'émetteur (18) individuelle n'est pas valable ou n'est pas contenue dans la liste d'autorisations (28).

2°) Procédé selon la revendication 1,
caractérisé en ce que
la liste d'autorisations (28) est enregistrée du côté de la réception dans une mémoire de l'appareil de commande (16).

3°) Procédé selon les revendications 1 ou 2,
caractérisé en ce qu'
une zone de mémoire (BSS, PS, DS) de la commande à programme en mémoire constituant l'appareil de commande (16) peut être commandée de manière précise par le codage du fichier à transmettre.

4°) Procédé selon la revendication 1,
caractérisé en ce que
la liste d'autorisations (28) est adaptable individuellement et toute manipulation de cette liste (28) n'est possible qu'avec des droits correspondants.

5°) Procédé selon la revendication 1,
caractérisé en ce que

les types de transmission et/ou les zones de mémoire (BSS, PS, DS) se définissent et lors d'une transmission de données à partir de l'appareil de traitement de données (16), on fait un codage avec une signature numérique (24) et/ou une clé publique et/ou privée (26).

6°) Procédé selon la revendication 1,
caractérisé en ce qu'
on code les données (10) du côté de l'émetteur avec une signature numérique (18) et une clé publique (20) et on décode les données (10) du côté de la réception avec une clé secrète (22) correspondante.

7°) Procédé selon la revendication 1,
caractérisé en ce qu'
on transmet les données (10) à l'état codé.

8°) Procédé selon la revendication 1,
caractérisé en ce qu'
on transmet les données (10) par un réseau de données (14) tel que le réseau Intranet ou Internet.

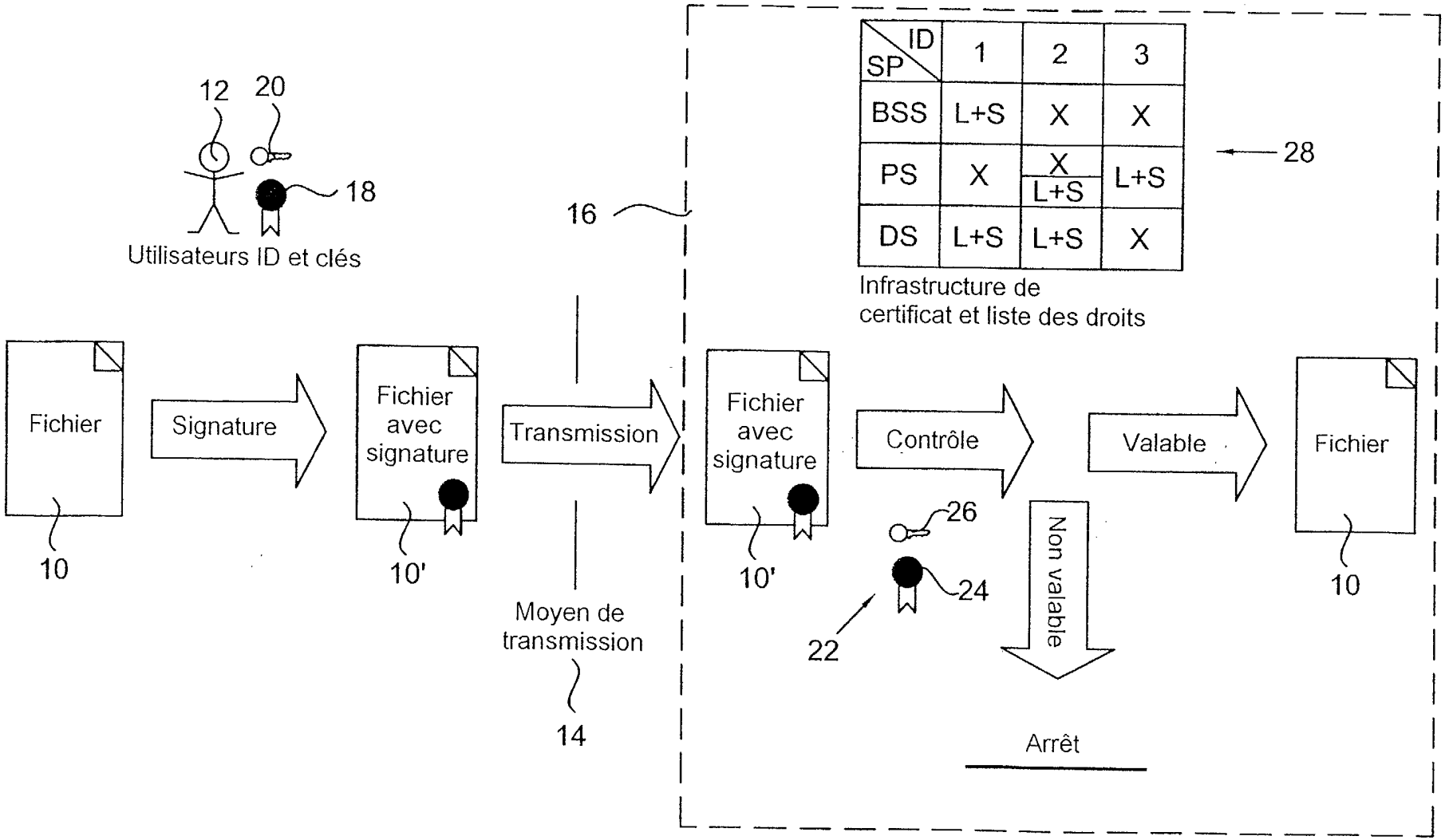
9°) Appareil de commande tel que commande à programme en mémoire,
caractérisé en ce que
l'appareil de commande (16) comporte une unité de réception avec une unité de décodage pour décoder au moins une caractéristique d'émetteur (18) des données reçues (10'),
l'appareil de commande (16) présente une liste d'autorisation (28) dans laquelle à différentes caractéristiques d'émetteur (ID 1... ID n) sont attribués des droits pour modifier l'état de l'appareil de commande (16), et
l'état de l'appareil de commande (16) peut être modifié pour une caractéristique d'émetteur (ID 1... ID n) valable et contenue dans la liste d'autorisations (28), en fonction des droits donnés par la liste d'autorisations (28).

10°) Appareil de commande selon la revendication 9,
caractérisé en ce que
l'appareil de commande (16) comporte une unité d'émission avec une installation de codage pour coder des données (10) à émettre, et dans

l'installation de codage, on a une signature numérique et/ou une clé publique pour coder les données.

11°) Appareil de commande selon la revendication 9 ou 10,
caractérisé en ce que
la zone de mémoire de la commande à programme en mémoire est subdivisée en zones définies librement (BSS, PS, DS) et pour chaque zone de mémoire (BSS, PS, DS) dans la liste d'autorisation (28), on définit des droits pour différentes caractéristiques d'émetteur (ID 1, ID 2, IDn).

12°) Appareil de commande selon la revendication 11,
caractérisé en ce qu'
il est une commande à programme enregistré en mémoire.


12
20
18
Utilisateurs ID et clés
16
ID / SP
1
2
3
BSS
L+S
X
X
PS
X
X
L+S
L+S
DS
L+S
L+S
X
28
Infrastructure de certificat et liste des droits
Fichier
10
Signature
Fichier avec signature
10'
Transmission
Moyen de transmission
14
Fichier avec signature
10'
Contrôle
26
24
22
Non valable
Valable
Fichier
10
Arrêt