MINISTERO DELLO SVILUPPO ECONOMICO
DIREZIONE GENERALE PER LA LOTTA ALLA CONTRAFFAZIONE
UFFICIO ITALIANO BREVETTI E MARCHI

UIBM

DOMANDA DI INVENZIONE NUMERO	**102022000003482**
Data Deposito	**24/02/2022**
Data Pubblicazione	**25/05/2022**

Classifiche IPC

Sezione	Classe	Sottoclasse	Gruppo	Sottogruppo
B	61	L	25	08

Sezione	Classe	Sottoclasse	Gruppo	Sottogruppo
B	61	L	27	30

Titolo

SISTEMA E METODO PER LA RAPPRESENTAZIONE DELLO STATO DI UN IMPIANTO FERROVIARIO IN UN TERMINALE OPERATORE DI TIPO COMMERCIALE SU RETE APERTA

Ing. Marco CONTI
(Albo iscr. n. 1280 BM)

DESCRIZIONE

Annessa a domanda di brevetto per INVENZIONE INDUSTRIALE avente per titolo

SISTEMA E METODO PER LA RAPPRESENTAZIONE DELLO STATO DI UN IMPIANTO FERROVIARIO IN UN TERMINALE OPERATORE DI TIPO COMMERCIALE SU RETE APERTA

A nome: **RFI S.p.A**.
Piazza della Croce Rossa, 1
00161 ROMA
Mandatari: Ing. Marco CONTI, Albo iscr. nr. 1280 BM

****

La presente invenzione ha per oggetto un sistema e un metodo per la rappresentazione di uno stato di un impianto ferroviario su un terminale di tipo commerciale connesso su rete aperta.

Per *rete aperta* si intende, come definito nella norma CENELEC EN 50159, un “sistema di trasmissione aperto – sistema di trasmissione con un numero sconosciuto di partecipanti, con proprietà sconosciute, variabili e non affidabili, utilizzato per servizi di telecomunicazione sconosciuti e con potenzialità di accesso non autorizzato”.

La presente descrizione riguarda il settore della rappresentazione in sicurezza dello stato di un impianto ferroviario o di parti di esso, ovvero enti ferroviari quali ad esempio segnali, deviatoi, circuiti di binario, passaggi a livello e altri; la presente descrizione riguarda inoltre il settore dell’inoltro, in sicurezza, di comandi per la gestione dello stato di un impianto ferroviario o di parti di esso, da parte di un operatore attraverso un terminale operatore di tipo commerciale connesso su rete aperta.

In particolare, in tale settore, sono in uso interfacce utente, ovvero sistemi di rappresentazione e di controllo, come nel caso dei cosiddetti *quadro luminoso* e *terminale operatore*, i quali permettono ad un operatore di

comprendere lo stato dell'impianto ferroviario e di impartire comandi per la gestione di tale impianto. In aggiunta o in sostituzione al quadro luminoso e al terminale operatore, che sono interfacce utente di tipo fisso, vi possono essere, interfacce utente mobili, quali ad esempio dispositivi *tablet*, comprendenti uno schermo per la visualizzazione e un sistema per impartire comandi. In questo settore tecnico, la sicurezza del segnalamento ferroviario è gestita da una piattaforma di controllo e comando, detta anche nucleo in sicurezza o *apparato centrale*, che è per un esempio del settore ferroviario preposta ad eseguire in sicurezza le logiche di instradamento o al distanziamento dei treni, al controllo di compatibilità tra i comandi inviati da un operatore e lo stato dell'impianto ferroviario, di modo che non sia possibile eseguire movimenti in conflitto tra loro; pertanto, al fine di garantire il corretto funzionamento del sistema, la piattaforma di controllo e comando deve rispondere a determinati requisiti di sicurezza; in particolare, nel settore ferroviario, tali sistemi sono sviluppati in conformità con lo standard di sicurezza Europeo CENELEC, e devono rispondere ai requisiti del livello SIL4 (*Safe Integrity Level 4*) definito nelle norme EN 50126, EN 50128 e EN 50129.

Allo stesso modo, è importante che i sistemi di rappresentazione e controllo per la gestione dell'impianto, ovvero le interfacce utente, rispettino uno standard di sicurezza sufficientemente elevato, in modo tale che le azioni dell'operatore siano svolte in modo sicuro e coerente con lo stato dell'impianto ferroviario.

Mentre esistono diversi metodi per raggiungere questo obiettivo con sistemi progettati allo scopo e connessi su reti chiuse, raggiungere lo stesso obiettivo è particolarmente complesso qualora si debbano utilizzare interfacce operatore che utilizzino dispositivi commerciali (COTS: *commercial off-the-shelf*) e connessi tramite rete aperta.

A tale fine, sono noti sistemi per la rappresentazione che impiegano procedure di verifica della correttezza e dell'integrità di informazioni e immagini riguardanti lo stato dell'impianto da visualizzare.

Un esempio di tali sistemi è contenuto in EP3438828B1, che descrive un sistema in cui la corretta rappresentazione dell'immagine è verificata mediante un controllo in retroazione tra un'immagine da visualizzare, generata da un dispositivo COTS, e dei dati, acquisiti da un nucleo in sicurezza, ovvero una piattaforma di controllo e comando, e a partire dai quali l'immagine è stata generata. Poiché la generazione dell'immagine avviene internamente ad un dispositivo COTS, le misure adottate per raggiungere uno standard di sicurezza sufficientemente elevato – e che comprendono l'adozione di meccanismi di retroazione – in questo caso rendono il sistema complesso e le sue prestazioni potenzialmente critiche.

Un ulteriore esempio è contenuto in ITGE2011000034, il quale descrive un sistema in cui un primo processore genera un'immagine e la manda ad uno schermo, dal quale un dispositivo *frame grabber* cattura l'immagine e la manda ad un secondo processore; il secondo processore genera una seconda immagine e la confronta l'immagine catturata dal *frame grabber*; pertanto anche in questo caso il controllo avviene in retroazione. Tuttavia, la presenza del dispositivo *frame grabber* ed il controllo in retroazione rendono il sistema complesso. Inoltre, questo sistema è difficilmente realizzabile su dispositivi portatili, ovvero mobili, connessi su rete aperta e non può impiegare terminali di tipo commerciale.

Scopo del presente trovato è rendere disponibile un sistema e un metodo per la rappresentazione stato di un impianto ferroviario mediante un terminale operatore COTS connesso su rete aperta che superino gli inconvenienti delle tecniche note sopra citate e che sia semplice da realizzare.

Detto scopo è pienamente raggiunto dal sistema e dal metodo, oggetto del presente trovato, che si caratterizza per quanto contenuto nelle rivendicazioni sotto riportate.

Il sistema comprende una piattaforma di controllo e comando, configurato per fornire un flusso di dati di ingresso. Il flusso di dati di ingresso è rappresentativo dello stato dell'impianto ferroviario o di parti dell'impianto

ferroviario, ovvero enti ferroviari quali ad esempio segnali, deviatoi, circuiti di binario, passaggi a livello e altri.

Il sistema comprende un terminale di calcolo, configurato per ricevere un flusso di dati di ingresso. In un esempio, il terminale di calcolo è conforme a requisiti prescritti per i massimi livelli di *safety integrity* come richiesti per applicazioni *safety-critical* e definiti dalle norme CENELEC EN 50128 ed EN 50129. Preferibilmente, il terminale di calcolo è configurato per ricevere il flusso di dati di ingresso dalla piattaforma di controllo e comando. Il terminale di calcolo è configurato per generare un flusso di prime immagini e un flusso di seconde immagini a partire dal flusso di dati di ingresso. Preferibilmente le immagini del flusso di prime immagini e del flusso di seconde immagini sono in un formato grezzo, ovvero un formato *raw,* e il terminale di calcolo è configurato per convertire le immagini del flusso di prime immagini e del flusso di seconde immagini dal formato *raw* ad un formato standard.

In particolare, il flusso di dati di ingresso include una pluralità di serie di dati, ciascuna serie di dati della pluralità di serie di dati è rappresentativa dello stato dell'impianto ferroviario o di parti dell'impianto ferroviario in un medesimo istante. Ciascuna immagine del flusso di prime immagini è generata a partire da una rispettiva serie di dati della pluralità di serie di dati. Similmente, ciascuna immagine del flusso di seconde immagini è generata a partire da una rispettiva serie di dati della pluralità di serie di dati.

In un esempio preferito, il terminale di calcolo include un primo processore. Il primo processore è programmato per generare un flusso di prime immagini. Preferibilmente, il primo processore è programmato per generare, a partire dal flusso di dati di ingresso, un flusso di prime immagini. Preferibilmente, il terminale di calcolo include un secondo processore. Il secondo processore è programmato per generare un flusso di seconde immagini. Preferibilmente, il secondo processore è programmato per generare, a partire dal flusso di dati di ingresso, un flusso di seconde immagini.

Preferibilmente, il primo processore e il secondo processore ricevono in ingresso il medesimo flusso di dati di ingresso per generare, parallelamente, il flusso di prime immagini e il flusso di seconde immagini, rispettivamente.

Quindi, a partire da ciascuna serie di dati della pluralità di serie di dati, il primo processore è programmato per generare una immagine, realizzando, in questo modo, un corrispondente flusso di prime immagini. Similmente, a partire da ciascuna serie di dati della pluralità di serie di dati, il secondo processore è programmato per generare una immagine, realizzando, in questo modo, un corrispondente flusso di seconde immagini.

Il primo processore è programmato per generare le immagini del flusso di prime immagini in formato *raw*. Il primo processore è altresì programmato per convertire ciascuna immagine dal formato *raw* ad un predeterminato formato standard, ad esempio, al formato jpeg, gif, png o bitmap. Il secondo processore è programmato per generare le immagini del flusso di seconde immagini in formato *raw*. Il secondo processore è altresì programmato per convertire ciascuna immagine dal formato *raw* ad un predeterminato formato standard, ad esempio, al formato jpeg, gif, png o bitmap.

Preferibilmente, il primo processore e il secondo processore sono programmati per generare le rispettive immagini (ovvero le prime immagini del flusso di prime immagini e le seconde immagini del flusso di seconde immagini, rispettivamente) in un formato *raw* e per convertire ciascuna immagine dal formato *raw* ad un predeterminato formato standard, ad esempio, al formato jpeg, gif, png o bitmap.

Preferibilmente, una prima immagine del flusso di prime immagini, generata a partire da una serie di dati della pluralità di serie di dati in ingresso e una corrispondente seconda immagine del flusso di seconde immagini, generata a partire dalla medesima serie di dati della pluralità di serie di dati, forma una coppia d'immagini. In particolare, ciascuna immagine del flusso di prime immagini e del flusso di seconde immagini, generata a partire dalla medesima serie di dati della pluralità di serie di dati, forma una coppia d'immagini. In questo modo, a partire dal flusso di prime immagini e dal

flusso di seconde immagini, il terminale di calcolo genera un flusso di coppie d'immagini.

Il primo processore e il secondo processore possono essere programmati per generare le rispettive immagini in un formato *raw*, eseguendo applicativi (ovvero software) conformi ai requisiti prescritti per i massimi livelli di *safety integrity* per applicazioni *safety-critical* (ad esempio applicativi conformi ai requisiti SIL4 secondo la norma CENELEC EN 50128) senza la necessità di utilizzare librerie grafiche commerciali.

Il terminale di calcolo è configurato per generare un flusso d'immagini di uscita, ad esempio, a partire dal flusso di prime o di seconde immagini. Il flusso d'immagini di uscita può essere destinato ad essere visualizzato, ad esempio da un terminale operatore. Il terminale operatore può essere realizzato da un dispositivo COTS. Il dispositivo COTS può essere connesso al terminale di calcolo tramite una rete aperta. In un esempio, la rete aperta può comprendere una tra le reti mobili 3G, 4G, LTE o 5G.

In un esempio, il terminale di calcolo è configurato per verificare che, per ciascuna coppia d'immagini formata da una prima immagine del flusso di prime immagini e una corrispondente seconda immagine del flusso di seconde immagini, la prima e la seconda immagine siano coerenti l'una con l'altra. Il terminale di calcolo può essere configurato, in risposta ad un esito positivo di detta verifica, per abilitare una trasmissione in uscita del flusso d'immagini di uscita. In altre parole, il terminale di calcolo verifica che, per ciascuna coppia d'immagini formata da una prima immagine del flusso di prime immagini e una seconda immagine del flusso di seconde immagini, la prima immagine sia coerente con la seconda immagine e viceversa ovvero verifica che le la prima immagine coincida con la seconda immagine e viceversa.

Il software che viene eseguito sul primo processore e sul secondo processore, compreso il software per la generazione delle immagini, è conforme ai requisiti prescritti per i massimi livelli di *safety integrity* per applicazioni *safety-critical* (per esempio SIL4 secondo la norma ferroviaria

CENELEC EN 50128), e quindi non utilizza librerie *commercial off-the-shelf* (COTS), e in particolare non utilizza le librerie grafiche COTS.

Per questo motivo e per la verifica di coerenza tra la prima e seconda immagine sopra descritta, il sistema risulta tutelato nei confronti di errori nel processo di generazione dell'immagine da parte di uno tra il primo processore e il secondo processore.

Un'immagine di uscita del flusso d'immagini di uscita, preferibilmente, mostra all'operatore, attraverso uno schermo, una vista grafica che riporta lo stato di un impianto ferroviario o lo stato di parti dell'impianto ferroviario, quali ad esempio la posizione di un deviatoio, l'aspetto di un segnale alto, ed altri.

In un esempio di realizzazione, il terminale di calcolo include un canale di comunicazione bi-direzionale. Preferibilmente, il canale bi-direzionale collega tra loro il primo processore e il secondo processore. Ad esempio, il canale bi-direzionale può essere configurato per condividere informazioni tra il primo processore e il secondo processore. In particolare, il primo ed il secondo processore sono programmati per verificare la corrispondenza di una rispettiva coppia d'immagini, formata da una prima immagine del flusso di prime immagini e una corrispondente seconda immagine del flusso di seconde immagini.

Ad esempio, il primo processore e il secondo processore si scambiano, ovvero condividono, informazioni, le quali possono includere, ad esempio, una prima e una seconda immagine. Pertanto, la verifica della coerenza tra immagini è effettuata in modo ridondante, ovvero la verifica della coerenza tra immagini è effettuata sia dal primo processore che dal secondo processore. Tale caratteristica costituisce pertanto un elemento a tutela della sicurezza del sistema.

Ad esempio, da detta verifica, il primo processore è programmato per generare un primo segnale di verifica, rappresentativo della coerenza della rispettiva coppia d'immagini. Ad esempio, da detta verifica, il secondo processore è programmato per generare un secondo segnale di verifica,

rappresentativo della coerenza della rispettiva coppia d'immagini. Preferibilmente, ciascun processore della coppia costituita da primo e secondo processore è programmato per verificare una rispettiva coppia di immagini, per generare un primo segnale di verifica e un secondo segnale di verifica, rispettivamente, ciascun primo e secondo segnale di verifica essendo rappresentativo della coerenza della rispettiva coppia d'immagini. In particolare, ciascun processore della coppia costituita da primo e secondo processore è programmato per verificare ciascuna coppia del flusso di coppie d'immagini. Conseguentemente, il primo processore e il secondo processore, generano, rispettivamente, un flusso di primi segnali di verifica e un flusso di secondi segnali di verifica.

In un esempio di realizzazione, il primo processore è programmato per derivare, a partire dalla prima immagine, una prima firma e le informazioni condivise tra il primo e il secondo processore includono la prima firma. In questo modo, il primo processore deriva un flusso di prime firme, a partire dal corrispondente flusso di prime immagini. In un esempio, il secondo processore è programmato per derivare, a partire dalla seconda immagine, una seconda firma e le informazioni condivise tra il primo e il secondo processore includono la seconda firma. In questo modo, il secondo processore deriva un flusso di seconde firme, a partire dal corrispondente flusso di seconde immagini. Preferibilmente, il primo e il secondo processore sono programmati per derivare, a partire dalla prima immagine e dalla seconda immagine, rispettivamente, una corrispondente prima e seconda firma, e le informazioni condivise tra il primo e il secondo processore includono la prima e la seconda firma, per ciascuna coppia d'immagini.

Poiché il primo processore e il secondo processore si scambiano tra loro le rispettive firme, questo fa sì che la verifica della coerenza tra le immagini non avvenga tramite la verifica delle immagini stesse, ma attraverso la verifica di coerenza delle firme derivate a partire dalle immagini, rendendo la verifica più rapida. Ad esempio, la firma di un'immagine può essere

derivata applicando all'immagine una funzione che identifica univocamente tale immagine. Ad esempio, tale funzione può essere una funzione HASH.

In un esempio di realizzazione, il terminale di calcolo è provvisto di un sistema operativo. Preferibilmente, il sistema operativo è un sistema operativo in tempo reale, ovvero un sistema operativo *real-time*. Il sistema operativo *real-time* garantisce il determinismo delle operazioni svolte sotto la propria supervisione. Il sistema operativo *real-time* può essere conforme ai requisiti prescritti per i massimi livelli di *safety integrity*, come richiesti per applicazioni *safety-critical* dalle norme CENELEC EN 50128 ed EN 50129.

Il terminale di calcolo può essere configurato per svolgere, sotto la supervisione del sistema operativo *real-time*, alcune operazioni per cui il primo processore e il secondo processore, ovvero il terminale di calcolo, sono programmati. Tali funzioni possono includere, ad esempio:

- la generazione del flusso di prime immagini e del flusso di seconde immagini nel formato *raw*,
- la conversione di ciascuna prima immagine e seconda immagine dal formato *raw* al predeterminato formato standard,
- la verifica della coerenza della coppia d'immagini e
- la trasmissione del flusso di immagini di uscita, ovvero delle immagini di uscita.

In un esempio di realizzazione, il sistema comprende un terminale operatore, ovvero un terminale operatore fruibile, ad esempio, da un operatore ferroviario. Il terminale operatore può includere un terminale fisso, come ad esempio un *computer* COTS, oppure un terminale mobile COTS, come ad esempio un *tablet o uno smartphone*. Preferibilmente, il terminale operatore include uno schermo per visualizzare un flusso d'immagini di uscita.

In un esempio di realizzazione, il sistema comprende un server di trasferimento. Il server di trasferimento ha lo scopo di trasferire dati, ad esempio il flusso di immagini di uscita, ad un terminale operatore, preferibilmente un terminale operatore COTS. In particolare, il server di

trasferimento ha lo scopo di fornire un ambiente di lavoro (*workspace*) protetto, ovvero un ambiente di lavoro in cui le comunicazioni verso il terminale operatore e a partire dal terminale operatore avvengono in maniera sicura e protetta da intrusioni, in particolar modo qualora il terminale operatore sia un dispositivo COTS. In un esempio il server di trasferimento è conforme ai requisiti di *security* applicabili, come richiesti nelle normative NIS-2016/1148.

In un esempio, il terminale di calcolo può essere configurato per criptare o, in aggiunta, per comprimere ciascuna immagine del flusso di immagini di uscita. Il terminale di calcolo può essere altresì configurato per trasmettere ciascuna immagine del flusso di immagini di uscita criptata, o in aggiunta, compressa al server di trasferimento. Il server di trasferimento può essere configurato per decriptare, o in aggiunta decomprimere, ciascuna immagine del flusso di immagini in uscita. Il server di trasferimento può essere configurato per rendere disponibile il flusso di immagini in uscita ad un terminale operatore COTS. Ad esempio, il server di trasferimento può essere configurato per rendere disponibile flusso di immagini in uscita ad un terminale operatore COTS, operativamente connesso al server di trasferimento, attraverso un collegamento di comunicazione, ad esempio disponibile almeno temporaneamente, ovvero disponibile almeno per il tempo necessario al completamento di una sessione di lavoro. A tale scopo, ad esempio, il terminale operatore COTS può essere configurato per connettersi al server di trasferimento mediante una procedura di autenticazione in rete, mediante la quale un operatore inserisce delle proprie credenziali di accesso, ovvero un nome utente e una password.

In un esempio, il sistema può includere un server di gestione, configurato per ricevere le credenziali di accesso da parte del terminale operatore e gestire la procedura di autenticazione in rete, abilitando il collegamento di comunicazione tra il terminale operatore e il server di trasferimento per il tempo necessario al completamento di una sessione di lavoro.

In un esempio di realizzazione, il server di trasferimento è un server di rete.

Ad esempio, il server di rete ha lo scopo di trasferire il flusso di immagini di uscita al terminale operatore COTS, attraverso una pagina web. In particolare, il server di rete può essere configurato per ricevere il flusso di immagini di uscita dal terminale di calcolo, per decifrare e decomprimere ciascuna immagine del flusso di immagini di uscita e per creare una pagina web contente un'immagine del flusso d'immagini di uscita corrispondente allo stato aggiornato dell'impianto. Il server di rete può essere configurato per trasmettere la pagina web al terminale operatore COTS, ad esempio tramite una connessione su rete aperta.

Il server di trasferimento ha lo scopo di trasferire flusso di immagini di uscita ad un dispositivo COTS, in modo da aumentare la sicurezza e la protezione del flusso di immagini di uscita.

In un esempio alternativo il server di trasferimento trasmette ciascuna immagine del flusso di immagini di uscita al terminale operatore COTS, il terminale operatore COTS essendo configurato per decomprimere e decriptare ciascuna immagine del flusso di immagini di uscita.

Il terminale operatore può includere un sistema di comando, configurato per comandare l'impianto ferroviario o parti dell'impianto ferroviario. Ad esempio, il sistema di comando può includere un monitor *touch screen*, e in aggiunta o in alternativa includere un mouse, e in aggiunta o in alternativa, una tastiera, i quali permettono all'operatore di interagire con il terminale operatore per impartire comandi. Il terminale operatore può essere connesso al terminale di calcolo e può comprendere un sistema di comando, per inviare un segnale di comando al terminale di calcolo, per comandare l'impianto ferroviario o parti dell'impianto ferroviario.

Il sistema può comprendere un sistema di autorizzazione, al fine di verificare e autorizzare i segnali di comando generati dal terminale operatore. A tale fine, il terminale di calcolo può essere configurato per ricevere un segnale di comando dal terminale operatore e generare, in risposta al segnale di comando, una *one-time password*. Il terminale di calcolo può essere altresì configurato per generare un segnale di richiesta

per il terminale operatore, ovvero un segnale di richiesta di un inserimento della *one-time password* da parte dell'operatore. Il terminale operatore può essere configurato per ricevere la *one-time password* dal terminale di calcolo. Il terminale operatore può essere configurato per ricevere dal terminale di calcolo il segnale di richiesta di inserimento della *one-time password*.

In risposta al segnale di richiesta di inserimento della *one-time password* da parte del terminale di calcolo, il terminale operatore può essere configurato per restituire la *one-time password* al terminale di calcolo. Preferibilmente, la trasmissione della *one-time password* dal terminale di calcolo al terminale operatore avviene attraverso un canale di comunicazione differente rispetto al canale di comunicazione utilizzato per la restituzione della *one-time password* dal terminale operatore al terminale di calcolo. In un esempio la trasmissione della *one-time-password* dal terminale di calcolo al terminale operatore avviene utilizzando la tecnologia SMS, mentre la restituzione della *one-time-password* al terminale di calcolo da parte del terminale operatore avviene utilizzando una connessione dati. In un altro esempio, la trasmissione e la restituzione della *one-time-password* avvengono su due canali differenti che utilizzano una medesima tecnologia, ad esempio che utilizzano una connessione dati, ma su connessioni differenti.

Preferibilmente, la trasmissione della *one-time password* dal terminale di calcolo al terminale operatore avviene attraverso un canale di comunicazione differente rispetto al canale di comunicazione in cui avviene la trasmissione del flusso di immagini di uscita dal terminale di calcolo al terminale operatore. In un ulteriore esempio, il sistema può comprendere un dispositivo mobile personale, ad esempio uno *smartphone* in dotazione all'operatore, connesso al terminale di calcolo per la trasmissione, attraverso un canale di comunicazione, della *one-time password*, mentre la restituzione della *one-time password* avviene attraverso un canale di comunicazione tra il terminale operatore, ad esempio un *tablet* o un *computer*, e il terminale di calcolo.

In un esempio la trasmissione della *one-time password* dal terminale di calcolo al terminale operatore e dal terminale operatore al terminale di calcolo è realizzata all'interno di un *workspace protetto* in cui viene trasmessa la totalità dei dati da e verso il terminale operatore, incluse le immagini, i comandi, i dati di autenticazione dell'utente, i dati di criptazione.

In un esempio, il terminale di calcolo è configurato per controllare che la *one-time password* generata dal terminale di calcolo, ovvero la *one-time password* trasmessa dal terminale di calcolo al terminale operatore e la *one-time password* restituita dal terminale operatore al terminale di calcolo siano coerenti l'una con l'altra. Nel caso che il controllo abbia esito positivo, il terminale di calcolo è configurato per trasmettere il segnale di comando alla piattaforma di controllo e comando in risposta a detto controllo, in modo che soltanto i comandi positivamente verificati siano inoltrati alla piattaforma di controllo e comando.

In un esempio, il terminale operatore COTS è programmato per generare e trasmettere al terminale di calcolo, in aggiunta al segnale di comando, un segnale di conferma del comando da parte dell'operatore. Il terminale di calcolo può essere programmato per ricevere il segnale di conferma del comando da parte dell'operatore e per trasmettere il segnale di comando alla piattaforma di controllo e comando, alla ricezione del segnale di conferma del comando.

In un esempio di realizzazione, il terminale di calcolo include un circuito *watch-dog*. Il circuito *watch-dog* è connesso al primo processore e al secondo processore. Il circuito *watch-dog* può essere conforme ai requisiti prescritti per i massimi livelli di *safety integrity*, come richiesti per applicazioni *safety-critical* dalle norme CENELEC EN 50128 ed EN 50129. Il circuito *watch-dog* è configurato per disabilitare la trasmissione del flusso di immagini di uscita, in risposta ad un esito negativo della verifica di coerenza di ciascuna coppia d'immagini del flusso di coppie di immagini generato dal primo e dal secondo processore. Ad esempio, il circuito *watch-dog* può essere connesso al primo processore per ricevere il primo segnale

di verifica dal primo processore e disabilitare la trasmissione dell'immagine in uscita, in risposta ad un esisto negativo della verifica della coppia d'immagini. Il circuito *watch-dog* può essere altresì connesso al secondo processore per ricevere il secondo segnale di verifica dal secondo processore e disabilitare la trasmissione dell'immagine di uscita. In una forma realizzativa preferita, il circuito *watch-dog* è connesso al primo processore e al secondo processore per ricevere, rispettivamente, il primo segnale di verifica e il secondo segnale di verifica e per disabilitare la trasmissione dell'immagine di uscita dal terminale di calcolo ad un esito negativo della verifica della coppia d'immagini, ovvero in risposta al primo segnale di verifica e al secondo segnale di verifica, in cui almeno uno dei segnali di verifica è rappresentativo di un esito negativo della verifica della coppia d'immagini. In questo modo, la trasmissione dell'immagine in uscita è garantita soltanto quando entrambi il primo e il secondo processore sono in accordo sulla verifica della congruenza della coppia d'immagini. Qualora almeno uno tra il primo processore e il secondo processore risultasse in disaccordo sulla verifica della coerenza della coppia d'immagini, o rilevasse qualunque altro tipo di anomalia con potenziale impatto sulla *safety* del sistema, il circuito *watch-dog* è programmato per disabilitare la trasmissione dell'immagine in uscita ed evitare che siano prese da parte dell'operatore decisioni potenzialmente pericolose, in conseguenza di una visualizzazione incoerente con lo stato dell'impianto.

La presente descrizione mette a disposizione anche un metodo per rappresentare uno stato di un impianto ferroviario.

Il metodo comprende una fase di predisposizione, da parte di una piattaforma di controllo e comando, di un flusso di dati di ingresso rappresentativi dello stato dell'impianto ferroviario. Il metodo comprende una fase di ricezione, ad un terminale di calcolo, di un flusso di dati di ingresso. In un esempio il terminale di calcolo è conforme ai requisiti prescritti per i massimi livelli di *safety integrity*, come richiesti per applicazioni *safety-critical* e definiti dalle norme CENELEC EN 50128 ed EN

50129. Il metodo prevede una fase di generazione, da parte del terminale di calcolo a partire da un flusso di dati di ingresso, di un flusso di prime immagini. Le immagini del flusso di prime immagini sono, ad esempio, in formato *raw*. Il metodo prevede una fase di generazione, da parte del terminale di calcolo, a partire da un flusso di dati di ingresso, di un flusso di seconde immagini. Le immagini del flusso di seconde immagini sono, ad esempio, in formato *raw*. Secondo un esempio, il metodo prevede una fase di conversione, da parte del terminale di calcolo, delle immagini del flusso di prime immagini dal formato *raw* ad un formato standard, il metodo può prevedere una fase di conversione, da parte del terminale di calcolo, di un flusso di seconde immagini dal formato *raw* ad un formato standard. Il metodo prevede una fase di verifica, da parte del terminale di calcolo, per ciascuna coppia d'immagini formata da una prima immagine di un flusso di prime immagini e da una corrispondente seconda immagine del flusso di seconde immagini, che la prima e la seconda immagine siano coerenti l'una con l'altra. In conseguenza di una fase di verifica, il metodo comprende una fase di trasmissione, da parte del terminale di calcolo, ovvero di abilitazione del terminale di calcolo alla trasmissione, del flusso d'immagini di uscita, ad esempio ottenuto a partire dal flusso di prime o di seconde immagini.

In un esempio preferito, il terminale di calcolo include un primo processore e un secondo processore. Il metodo comprende una fase di ricezione, al terminale di calcolo, del flusso di dati di ingresso. Il metodo comprende una fase di generazione, da parte del primo processore, a partire dal flusso di dati di ingresso, di un flusso di prime immagini. Preferibilmente, le immagini del flusso di prime immagini sono in un formato *raw*. Preferibilmente, il metodo comprende una ulteriore fase di generazione, da parte del secondo processore, a partire dal flusso di dati di ingresso, di un flusso di seconde immagini. Preferibilmente, le immagini del flusso di seconde immagini sono in un formato *raw*. Il metodo comprende una fase di conversione, da parte del primo processore e del secondo processore, delle rispettive immagini dal formato *raw* ad un formato standard. Il metodo può prevedere una fase

di verifica, da parte del primo processore e del secondo processore, per ciascuna coppia d'immagini formata da una prima immagine del flusso di prime immagini e da una corrispondente seconda immagine del flusso di seconde immagini, che la prima e la seconda immagine siano coerenti l'una con l'altra. In conseguenza di una fase di verifica, il metodo può prevedere una fase di abilitazione alla trasmissione di un flusso di immagini in uscita, da parte del terminale di calcolo, ottenuto a partire dal flusso di prime o di seconde immagini. In un esempio, il primo e il secondo processore eseguono applicativi conformi ai requisiti prescritti per i massimi livelli di *safety integrity* per applicazioni *safety-critical* e definiti dalle norme CENELEC EN 50128 senza la necessità di utilizzare librerie grafiche commerciali per la generazione delle immagini.

In una forma realizzativa, il terminale di calcolo include un canale di comunicazione bi-direzionale tra il primo processore e il secondo processore, e il metodo può comprendere una fase di condivisione di informazioni tra il primo processore e il secondo processore, attraverso il canale bi-direzionale. Il metodo può comprendere una fase di verifica, da parte del primo e del secondo processore, di una rispettiva coppia d'immagini. Il metodo può inoltre prevedere una fase di generazione, da parte del primo e del secondo processore, di un primo segnale di verifica e di un secondo segnale di verifica, rispettivamente, ciascun segnale di verifica essendo rappresentativo di una coerenza della rispettiva coppia d'immagini.

Secondo una forma realizzativa, il metodo comprende una fase di derivazione, da parte del primo e del secondo processore, a partire dalla prima immagine e dalla seconda immagine, rispettivamente, di una corrispondente prima firma e seconda firma. Preferibilmente, il metodo comprende una fase di condivisione di informazioni tra il primo e il secondo processore, la fase includendo la condivisione della prima e della seconda firma, per ciascuna coppia d'immagini.

In un esempio di realizzazione, il metodo comprende una fase di

interruzione, da parte di un circuito *watch-dog,* ad esempio conforme ai requisiti prescritti per i massimi livelli di *safety integrity* per applicazioni *safety-critical* dalle norme CENELEC EN 50128 ed EN 50129, della trasmissione del flusso di immagini di uscita. Preferibilmente, il metodo comprende una fase di interruzione, da parte di un circuito *watch-dog*, della trasmissione del flusso di immagini di uscita in risposta ad un esito negativo della verifica. Ad esempio, il metodo può prevedere una fase di ricezione, al circuito *watch-dog*, di un primo segnale di verifica e di un secondo segnale di verifica e una fase di interruzione della trasmissione del flusso di immagini di uscita in risposta ad un esito negativo della verifica della coppia d'immagini, ovvero in risposta ad almeno uno tra il primo segnale di verifica e il secondo segnale di verifica negativo, ovvero rappresentativo di un esito negativo della verifica della coppia d'immagini da parte del primo processore o da parte del secondo processore.

In una forma realizzativa, il metodo prevede una predisposizione di un server di trasferimento, il server di trasferimento provvedendo uno spazio di lavoro (*workspace*) protetto, preferibilmente, nel caso in cui il terminale operatore includa un dispositivo COTS, ovvero un ambiente in cui le comunicazioni verso il terminale operatore e a partire dal terminale operatore avvengono in maniera sicura e protetta da intrusioni. In un esempio, il server di trasferimento è realizzato in conformità con requisiti di *security* che garantisce le caratteristiche di *security* richieste dalle normative NIS-2016/1148ad esempio secondo le normative NIS-2016/1148. A tale scopo, il metodo può prevedere una fase di criptazione, o in aggiunta, di compressione, ad esempio da parte del terminale di calcolo, di ciascuna immagine del flusso di immagini di uscita. Il metodo può comprendere una fase di trasferimento, da parte del terminale di calcolo, del flusso di immagini di uscita, ad esempio al server di trasferimento. Il metodo può comprendere una fase di decriptazione, o in aggiunta di decompressione, da parte del server di trasferimento, di ciascuna immagine del flusso di immagini di uscita. Il metodo può prevedere la predisposizione di un terminale operatore

COTS, ad esempio operativamente connesso al server di trasferimento, attraverso un collegamento di comunicazione, disponibile almeno temporaneamente, ovvero disponibile almeno per un tempo necessario al completamento di una sessione di lavoro. Ad esempio il terminale operatore COTS può essere configurato per connettersi al server di trasferimento mediante una procedura di autenticazione in rete, tramite la quale un operatore inserisce delle credenziali di accesso, ovvero un nome utente e una password. In un esempio, il metodo può prevedere una fase di autenticazione in rete, da parte di un server di gestione. L'autenticazione in rete può prevedere una fase di ricezione delle credenziali di accesso provenienti dal terminale operatore e una fase di verifica delle credenziali per abilitare il collegamento di comunicazione tra il terminale operatore e il server di trasferimento almeno per il tempo necessario al completamento di una sessione di lavoro.

Il metodo può prevedere una fase di alimentazione, al terminale operatore COTS, da parte del server di trasferimento, del flusso di immagini di uscita. Il metodo può comprendere una fase di visualizzazione, da parte del terminale operatore COTS, di ciascuna immagine del flusso di immagini di uscita.

In una forma realizzativa, il metodo comprende una fase, eseguita da parte di un terminale operatore, di comando dell'impianto o di parti dell'impianto ferroviario. A tale scopo, il metodo può prevedere una fase di invio di un segnale di comando da parte del terminale operatore. Il terminale operatore può essere un terminale operatore COTS, ad esempio un *tablet* o un *computer*. Il metodo può prevedere una fase di ricezione, da parte del terminale di calcolo, di un segnale di comando da parte di un terminale operatore COTS. Il metodo può includere una fase di generazione di una *one-time password*, da parte del terminale di calcolo, in risposta al segnale di comando. Il metodo può prevedere un'ulteriore fase di generazione di un segnale di richiesta per il terminale operatore COTS, da parte del terminale di calcolo, ovvero di un segnale di richiesta di un inserimento della *one-time*

password da parte di un operatore. Il metodo può prevedere una fase di ricezione della *one-time password*, da parte del terminale operatore COTS. Inoltre, il metodo può includere una fase di restituzione della *one-time password* al terminale di calcolo in risposta al segnale di richiesta di inserimento della *one-time password* da parte del terminale di calcolo. Preferibilmente, il metodo può comprendere un'ulteriore fase, da parte del terminale di calcolo, di controllo che la *one-time password* generata dal terminale di calcolo, ovvero la *one-time password* trasmessa dal terminale di calcolo al terminale operatore COTS e la *one-time password* restituita dal terminale operatore COTS siano coerenti l'una con l'altra. Il metodo può altresì prevedere una fase, eseguita dal terminale di calcolo, di trasmissione del segnale di comando alla piattaforma di controllo e comando, in caso di verifica positiva di detto controllo.

In un esempio, il metodo comprende una fase, tramite il terminale di calcolo, di ricezione di un segnale di comando dal terminale operatore COTS. Il metodo può comprendere delle fasi, tramite il terminale operatore COTS, di generazione e trasmissione del segnale di comando al terminale di calcolo, di generazione e trasmissione, al terminale di calcolo, di un segnale di conferma del comando da parte di un operatore, e, tramite il terminale di calcolo, delle fasi di ricezione del segnale di conferma del comando da parte dell'operatore e di trasmissione del segnale di comando alla piattaforma di controllo e comando, alla ricezione di detto segnale di conferma. In un esempio, la trasmissione del segnale di conferma del segnale di comando avviene tramite il server di trasferimento, sulla base delle funzioni di *security* offerte dal workspace protetto.

Il sistema secondo il presente trovato è conforme ai più stringenti requisiti di *safety* per applicazioni *safety-critical* e di *security*, e permette di raggiungere i seguenti scopi:

- rappresentare in modo sicuro lo stato di un impianto ferroviario su un terminale per interfaccia operatore, eventualmente anche di tipo commerciale (compresi i dispositivi *tablet*), collegato tramite rete aperta

(comprese le reti mobili 3G/4G/LTE/5G) ad un sistema di elaborazione, che riceve lo stato dell'impianto ferroviario da una piattaforma di controllo e comando;

- inoltrare dal terminale operatore comandi verso la piattaforma di controllo e comando.

La protezione della trasmissione dei dati su rete aperta (*security*) è garantita da una piattaforma protetta (*server di trasferimento*), che preferibilmente è conforme alle normative NIS-2016/1148, per il controllo degli accessi e l'indirizzamento verso la piattaforma di controllo e comando dell'impianto ferroviario, per la decodifica (decriptazione) e decompressione delle immagini e per ogni altro tipo di comunicazione da e per il terminale.

Il Livello di Integrità della Sicurezza (*Safety Integrity Level, SIL*) è particolarmente elevato, grazie anche all'architettura del terminale di calcolo, che preferibilmente è conforme ai requisiti definiti dalle norme CENELEC EN 50128 ed EN 50129; un altro aspetto che contribuisce a mantenere elevato il Livello di Integrità della Sicurezza è rappresentato dalla decodifica (decriptazione) sul terminale operatore dell'immagine codificata (criptata) dal terminale di calcolo prima della trasmissione.

Si osservi che il sistema secondo la presente descrizione può essere impiegato anche in tutte le applicazioni industriali diverse da quelle ferroviarie, in cui sia necessario remotizzare in sicurezza un generico terminale di interfaccia operatore.

Questa ed altre caratteristiche risulteranno maggiormente evidenziate dalla descrizione seguente di una preferita forma realizzativa, illustrata a puro titolo esemplificativo e non limitativo nelle unite tavole di disegno, in cui:

- la figura 1 illustra un sistema per rappresentare uno stato di un impianto ferroviario, secondo uno o più degli aspetti della presente descrizione;
- la figura 2 illustra un sistema per rappresentare uno stato di un impianto ferroviario su un terminale operatore COTS; secondo uno o più degli aspetti della presente descrizione;
- la figura 3 e la figura 4 illustrano un particolare del sistema secondo uno o

più degli aspetti della presente descrizione;

- le figure 5, 6 e 7 illustrano fasi del sistema per rappresentare uno stato di un impianto ferroviario, secondo uno o più degli aspetti della presente descrizione.

Nelle figure, si è indicato con 1 un sistema per rappresentare uno stato di un impianto ferroviario.

Il sistema 1 comprende una piattaforma di controllo e comando 10 e un terminale di calcolo 2. Il terminale di calcolo 2 è conforme ai requisiti prescritti per i massimi livelli di *safety integrity* come richiesti per applicazioni *safety-critical,* dalle normative CENELEC EN 50128 ed EN 50129. La piattaforma di controllo e comando 10 è configurata per fornire un flusso di dati di ingresso 100 al terminale di calcolo 2. A tale scopo, la piattaforma di controllo e comando 10 è connessa al terminale di calcolo 2 ad esempio attraverso una rete chiusa, ad esempio una rete LAN. Il flusso di dati di ingresso 100 è rappresentativo dello stato dell'impianto ferroviario o di parti dell'impianto ferroviario, ovvero enti ferroviari quali ad esempio segnali, deviatoi, circuiti di binario, passaggi a livello e altri. In particolare, il flusso di dati di ingresso 100 include una pluralità di serie di dati. Ciascuna serie di dati della pluralità di serie di dati è rappresentativa dello stato dell'impianto ferroviario o di parti di esso in un medesimo istante.

Il terminale di calcolo 2 è configurato per ricevere il flusso di dati di ingresso 100 dalla piattaforma di controllo e comando 10.

Il terminale di calcolo 2 è configurato per generare, a partire dal flusso di dati in ingresso 100, un flusso di prime immagini 201A. In particolare, ciascuna prima immagine 201A del flusso di prime immagini 201A è generata a partire da una rispettiva serie di dati della pluralità di serie di dati.

Il terminale di calcolo 2 è altresì configurato per generare, a partire dal flusso di dati in ingresso 100, un flusso di seconde immagini 201B. In particolare, ciascuna seconda immagine 201B del flusso di seconde immagini 201B è generata a partire da una rispettiva serie di dati della pluralità di serie di dati.

Quindi, a partire da ciascuna serie di dati della pluralità di serie di dati, il

terminale di calcolo 2 è programmato per generare una prima immagine 201A, realizzando, in questo modo, un corrispondente flusso di prime immagini 201A. Similmente, a partire da ciascuna serie di dati della pluralità di serie di dati, il terminale di calcolo 2 è programmato per generare una seconda immagine 201B, realizzando, in questo modo, un corrispondente flusso di seconde immagini 201B.

In un esempio preferito, il terminale di calcolo 2 include un primo processore 200A e un secondo processore 200B. Il primo processore 200A è programmato per generare, a partire dal flusso di dati di ingresso 100 al terminale di calcolo 2, un flusso di prime immagini 201A. Il secondo processore 200B è programmato per generare, a partire dal flusso di dati di ingresso 100 al terminale di calcolo 2, un flusso di seconde immagini 201B. Pertanto, il primo processore 200A e il secondo processore 200B sono programmati per generare, in parallelo, il flusso di prime immagini 201A e il flusso di seconde immagini 201B, rispettivamente. In particolare, il primo processore 200A è programmato per generare una immagine a partire da una serie di dati della pluralità di serie di dati del flusso di dati di ingresso 100, realizzando, in questo modo, il corrispondente flusso di prime immagini 201A. Similmente, il secondo processore 201B è programmato per generare una immagine a partire una serie di dati della pluralità di serie di dati del flusso di dati di ingresso 100, realizzando, in questo modo, il corrispondente flusso di seconde immagini 201B.

In un esempio, il primo processore 200A e il secondo processore 200B sono programmati per eseguire applicativi conformi ai requisiti prescritti per i massimi livelli di *safety integrity*per applicazioni *safety-critical*, secondo le normative CENELEC EN 50128 senza la necessità di utilizzare librerie grafiche commerciali. e, preferibilmente, sotto la supervisione di un sistema operativo in tempo reale. Il sistema operativo in tempo reale può essere conforme ai requisiti prescritti per i massimi livelli di *safety integrity* per applicazioni *safety-critical*, secondo le normative CENELEC EN 50128.

Il primo processore 200A e il secondo processore 200B sono programmati

per generare le rispettive immagini (ovvero le prime immagini 201A del flusso di prime immagini 201A e le seconde immagini 201B del flusso di seconde immagini 201B, rispettivamente) in un formato *raw* e per convertire ciascuna immagine dal formato *raw* ad un predeterminato formato standard, ovvero, ad esempio, al formato jpeg, gif, png o bitmap.

Ciascuna immagine del flusso di prime immagini 201A e del flusso di seconde immagini 201B, generata a partire dalla medesima serie di dati della pluralità di serie di dati del flusso di dati di ingresso 100, forma una coppia d'immagini; in questo modo, a partire dal flusso di prime immagini 201A e dal flusso di seconde immagini 201B, il terminale di calcolo 2 genera un flusso di coppie d'immagini.

Secondo una forma realizzativa, il primo processore 200A è programmato per derivare, a partire da ciascuna immagine del flusso di prime immagini 201A, un corrispondente flusso di prime firme 202A. Il secondo processore 200B è programmato per derivare, a partire da ciascuna immagine del flusso di seconde immagini 201B, un corrispondente flusso di seconde firme 202B. Ad esempio, ciascuna firma del flusso di prime firme 202A e del flusso di seconde firme 202B è derivata applicando, a ciascuna immagine del flusso di prime immagini 201A e del flusso di seconde immagini 201B, una medesima funzione, ad esempio una funzione HASH.

Preferibilmente, il terminale di calcolo 2 include un canale bidirezionale 203, il quale collega tra loro il primo processore 200A e il secondo processore 200B. In particolare, il canale bi-direzionale 203 realizza una *comunicazione tra processi* (*inter-process communication*: IPC) per consentire la condivisione di informazioni tra il primo processore 200A e il secondo processore 200B.

In particolare, attraverso il canale bi-direzionale 203, il primo processore 200A e il secondo processore 200B si scambiano, ovvero condividono tra loro, rispettivamente, il flusso di prime firme 202A e il flusso di seconde firme 202B. Ciascun processore della coppia costituita dal primo processore 200A e dal secondo processore 200B è programmato per verificare la

coerenza di ciascuna coppia d'immagini, confrontando ciascuna prima firma 202A del flusso di prime firme 202A con una corrispondente seconda firma 202B del flusso di seconde firme 202B. Il primo processore 200A è programmato per generare un primo segnale di verifica 204A, rappresentativo della coerenza di una prima firma 202A con una corrispondente seconda firma 202B, ovvero di una prima firma 202A derivata a partire da una prima immagine 201A del flusso di prime immagini 201A e una corrispondente seconda firma 202B derivata a partire da una seconda immagine 201B del flusso di seconde immagini 201B. Il primo processore 200A è programmato per generare un primo segnale di verifica 204A per ciascuna coppia d'immagini del flusso di coppie d'immagini, in modo tale da generare un corrispondente flusso di primi segnali di verifica 204A.

Similmente, il secondo processore 200B è programmato per generare un secondo segnale di verifica 204B, rappresentativo della coerenza di una prima firma 202A con una corrispondente seconda firma 202B, ovvero di una prima firma 202A derivata a partire da una prima immagine 201A del flusso di prime immagini 201A e una corrispondente seconda firma 202B derivata a partire da una seconda immagine 201B del flusso di seconde immagini 201B. Il secondo processore 200B è programmato per generare un secondo segnale di verifica 204B per ciascuna coppia d'immagini del flusso di coppie d'immagini, in modo tale da generare un corrispondente flusso di secondi segnali di verifica 204B.

In un esempio di realizzazione, il terminale di calcolo 2 include un circuito *watch-dog* 205. Il circuito watch-dog 205, preferibilmente, è realizzato secondo i requisiti prescritti per i massimi livelli di *safety integrity*, richiesti per applicazioni *safety-critical* secondo le normative CENELEC EN 50128 ed EN 50129. Il circuito *watch-dog* 205 è connesso al primo processore 200A e al secondo processore 200B per ricevere ciascun primo segnale di verifica 204A del flusso di primi segnali di verifica 204A dal primo processore 200A e il secondo segnale di verifica 204B del flusso di secondi

segnali di verifica 204B dal secondo processore 200B. In particolare, ciascun segnale di verifica del primo segnale di verifica 204A e del secondo segnale di verifica 204B può avere esito positivo, in risposta ad un esito positivo della coerenza di una coppia d'immagini, ovvero in risposta ad un esito positivo della coerenza di una coppia di firme, la coppia di firme essendo formata da una prima firma 202A e una corrispondente seconda firma 202B. Oppure, ciascun segnale di verifica del primo segnale di verifica 204A e del secondo segnale di verifica 204B può avere esito negativo, in risposta ad un esito negativo della coerenza della coppia d'immagini.

In caso di esito positivo del primo segnale di verifica 204A e del secondo segnale di verifica 204B, il terminale di calcolo 2 è configurato per trasmettere, a partire dal flusso di prime immagini 201A o dal flusso di seconde immagini 201B, un flusso di immagini di uscita 206. Nel caso in cui almeno un segnale di verifica tra il primo segnale di verifica 204A generato dal primo processore 200A e il secondo segnale di verifica 204B generato dal secondo processore 200B abbia esito negativo, il circuito *watch-dog* 205 è programmato per interrompere la trasmissione del flusso di immagini di uscita 206 da parte del terminale di calcolo 2.

In un esempio di realizzazione, il sistema 1 comprende un terminale operatore 3. Ad esempio, il terminale operatore 3 può essere un terminale fisso, come ad esempio un *computer*, oppure un terminale mobile, ovvero un dispositivo mobile, come ad esempio un *tablet*. Il terminale operatore include uno schermo 300, per trasmettere il flusso di immagini di uscita 206. Il terminale operatore 3 può essere un terminale operatore COTS. In un esempio di realizzazione in cui il terminale operatore 3 è un terminale operatore COTS, il sistema 1 comprende un server di trasferimento 4. Il server di trasferimento 4 è connesso al terminale di calcolo 2 e al terminale operatore COTS 3. Il server di trasferimento 4 ha lo scopo di fornire un *workspace* protetto, ovvero un ambiente in cui le comunicazioni tra il terminale di calcolo 2 e il terminale operatore COTS 3 avvengono in maniera sicura e protetta da intrusioni. Il *workspace* protetto, ovvero il

server di riferimento, in un esempio è conforme a requisiti di *security*, richiesti secondo le normative NIS-2016/1148. In una forma realizzativa, il server di trasferimento 4 è un server di rete. Il terminale di calcolo 2 è configurato per criptare e per comprimere ciascuna immagine del flusso di immagini di uscita 206; il terminale di calcolo 2 è configurato per trasmettere il flusso di immagini di uscita 206 criptato e compresso al server di trasferimento 4. Il server di trasferimento 4 è configurato per decriptare e per decomprimere il flusso di immagini di uscita 206 ricevuto dal terminale di calcolo 2. Il server di trasferimento 4 è configurato per rendere disponibile il flusso di immagini di uscita 206 al terminale operatore COTS 3. In un esempio, il server di trasferimento 4 è un server di rete. Il server di rete è configurato per decriptare e per decomprimere flusso di immagini in uscita 206 e generare una pagina web contenente ciascuna immagine del flusso di immagini di uscita 206. Il server di rete è inoltre configurato per trasmettere la pagina web al terminale operatore COTS 3 per essere visualizzata sullo schermo 300 del terminale operatore COTS 3.

In un esempio di realizzazione, il terminale operatore 3 include un sistema di comando 301, configurato per comandare l'impianto ferroviario o parti dell'impianto ferroviario. In un esempio, il terminale operatore 3 è un terminale operatore mobile, ad esempio un *tablet*, e il sistema di comando 301 può includere una tastiera 302, attraverso la quale l'operatore può interagire per generare un segnale di comando. In un esempio, Il terminale operatore 3 può essere un terminale operatore fisso, ad esempio un *computer*, e il sistema di comando 301 include una tastiera 302 e un mouse 303, attraverso i quali un operatore può interagire per comunicare con il terminale operatore 3. In un esempio, il terminale operatore 3 è connesso al terminale di calcolo 2 e comprende un sistema di comando 301 per inviare un segnale di comando 304 al terminale di calcolo 2.

In una forma realizzativa, il terminale di calcolo 2 può essere configurato per ricevere il segnale di comando 304 dal terminale operatore 3 e generare, in risposta al segnale di comando 304, una *one-time password*

306. Il terminale di calcolo 2 può essere inoltre configurato per generare un segnale di richiesta 307 di un inserimento della *one-time password* 306 per il terminale operatore 3, ovvero un segnale di richiesta di un inserimento della *one-time password* 306 da parte di un operatore al terminale operatore 3. Il terminale operatore 3 è configurato per ricevere dal terminale di calcolo 2 la *one-time password* 306 e il segnale di richiesta 307 di inserimento della *one-time password* 306. Il terminale operatore 3 è configurato per restituire la *one-time password* al terminale di calcolo 2, in risposta al segnale di richiesta 307 di inserimento della *one-time password* 306 da parte del terminale di calcolo 2. Preferibilmente, la trasmissione della *one-time password* 306 dal terminale di calcolo 2 al terminale operatore 3 avviene attraverso un canale di comunicazione differente rispetto al canale di comunicazione in cui avviene la trasmissione del flusso di immagini di uscita 206 dal terminale di calcolo 2 al terminale operatore 3. In particolare, il sistema 1 può comprendere un dispositivo mobile personale 308, ad esempio uno *smartphone* in dotazione all'operatore. Il dispositivo mobile personale 308 è connesso al terminale di calcolo 2 per la trasmissione della *one-time password* 306. La restituzione della *one-time password* 306 dal terminale operatore 3 al terminale di calcolo 2 avviene attraverso un canale di comunicazione tra il terminale operatore 3 e il terminale di calcolo 2. Preferibilmente, il terminale di calcolo 2 è configurato per controllare che la *one-time password* 306 generata dal terminale di calcolo 2, ovvero la *one-time password* 306 trasmessa dal terminale di calcolo 2 al dispositivo mobile personale 308, sul quale l'operatore legge la *one-time password*, e la *one-time password* 306 inserita dall'operatore e quindi restituita dal terminale operatore 3 al terminale di calcolo 2 siano coerenti l'una con l'altra. Nel caso che il controllo abbia esito positivo, ovvero la password trasmessa e la password restituita siano coerenti l'una con l'altra, il terminale di calcolo 2 è configurato per trasmettere, ovvero inoltrare, il segnale di comando 304 alla piattaforma di controllo e comando 10 in risposta a detto controllo.

In un esempio, il terminale operatore COTS (3) è programmato per

generare e trasmettere al terminale di calcolo (2), in aggiunta al segnale di comando (304), un segnale di conferma del comando da parte dell'operatore e il terminale di calcolo (2) è ulteriormente programmato per ricevere il segnale di conferma del comando da parte dell'operatore e per trasmettere il segnale di comando (304) alla piattaforma di controllo e comando (10), alla ricezione del segnale di conferma del comando.

Con riferimento alla figura 1 e alla figura 2, la piattaforma di controllo e comando 10 comprende uno stadio di:

- alimentazione, ovvero trasmissione, del flusso di dati di ingresso 100, rappresentativi dello stato dell'impianto ferroviario (stadio 10.A).

Il terminale di calcolo 2 comprende i seguenti stadi:

- generazione delle immagini a partire dal flusso di dati di ingresso 100 (stadio 2.A);
- consolidamento delle immagini (stadio 2.B);
- generazione di un flusso di immagini di uscita 206 a partire dalle immagini consolidate (stadio 2.C)
- trasmissione del flusso di immagini di uscita 206.

Il terminale operatore 3 comprende i seguenti stadi:

- ricezione del flusso di immagini di uscita 206 e visualizzazione di ciascuna immagine del flusso di immagini di uscita 206 (stadio 3.A).

In una forma realizzativa in cui il terminale operatore 3 è un terminale operatore COTS, il sistema 1 comprende un server di trasferimento 4, il terminale di calcolo 2 comprende un ulteriore stadio di:

- criptazione e compressione del flusso di immagini di uscita 206 e trasmissione al server di trasferimento 4 (stadio 2.D),

e il server di trasferimento 4 comprende i seguenti stadi:

- decriptazione e decompressione del flusso di immagini di uscita 206 (stadio 4.A);
- preparazione ed aggiornamento di una pagina web contenente ciascuna immagine del flusso di immagini in uscita e invio della pagina web al terminale operatore COTS 3 per la visualizzazione (stadio 4.B).

Il presente trovato mette a disposizione anche un metodo per rappresentare uno stato di un impianto ferroviario. Questo metodo è preferibilmente implementato in un sistema 1 per rappresentare lo stato di un impianto ferroviario, secondo una o più caratteristiche descritte sopra.

Preferibilmente, il metodo per rappresentare lo stato di un impianto ferroviario comprende le seguenti fasi, eseguibili in sequenza (illustrate a titolo di esempio nelle figure 5-7).

A0. Predisposizione di una piattaforma di controllo e comando 10 e di un terminale di calcolo 2 conforme ai requisiti prescritti per i massimi livelli di *safety integrity* per applicazioni *safety-critical* e definiti dalle norme CENELEC EN 50128 ed EN 50129, il terminale di calcolo 2 includendo un primo processore 200A e un secondo processore 200B. Predisposizione, da parte della piattaforma di controllo e comando 10, di un flusso di dati di ingresso 100, rappresentativi dello stato dell'impianto ferroviario e trasmissione, preferibilmente attraverso una rete chiusa, ad esempio una rete LAN, del flusso di dati di ingresso 100, da parte della piattaforma di controllo e comando 10.

A1. Ricezione, da parte del terminale di calcolo 2 del flusso di dati di ingresso 100 e ricezione, da parte di ciascun primo processore 200A e secondo processore 200B del flusso di dati di ingresso 100. Generazione, in parallelo da parte del primo processore 200A e del secondo processore 200B, a partire dal flusso di dati di ingresso 100, di un flusso di prime immagini 201A e un flusso di seconde immagini 201B, rispettivamente, in formato *raw*. Conversione, da parte del processore 200A e del secondo processore 200B delle rispettive immagini dal formato *raw* ad un formato standard, ad esempio jpeg, gif, png o bitmap. Ciascuna immagine del flusso di prime immagini 201A e del flusso di seconde immagini 201B, generata a partire dalla medesima serie di dati della pluralità di serie di dati del flusso di dati di ingresso 100, forma una coppia d'immagini in modo da formare un flusso di coppie d'immagini.

A2. Derivazione, da parte del primo processore 200A e del secondo

processore 200B, a partire da ciascuna immagine del flusso di prime immagini 201A e del flusso di seconde immagini 201B, rispettivamente, di un corrispondente flusso di prime firme 202A e un flusso di seconde firme 202B; il flusso di prime firme 202A e il flusso di seconde firme 202B è derivato applicando, a ciascuna immagine del flusso di prime immagini 201A e del flusso di seconde immagini 201B, una medesima funzione, ad esempio una funzione HASH.

A3. Scambio, ovvero condivisione, tra il primo processore 200A e il secondo processore 200B, attraverso un canale di comunicazione bi-direzionale 203, rispettivamente, del flusso di prime firme 202A e del flusso di seconde firme 202B.

A4. Verifica della coerenza, da parte del primo processore 200A e del secondo processore 200B, di ciascuna coppia d'immagini mediante il confronto di ciascuna prima firma 202A del primo flusso di prime firme 202A con una corrispondente seconda firma 202B del flusso di seconde firme 202B. Generazione, da parte del primo processore 200A e del secondo processore 200B, rispettivamente, di un primo segnale di verifica 204A e di un secondo segnale di verifica 204B, rispettivamente, per ciascuna coppia d'immagini del flusso di coppie d'immagini, in modo tale da generare un corrispettivo flusso di primi segnali di verifica 204A e secondi segnali di verifica 204B. Il primo segnale di verifica 204A e il secondo segnale di verifica 204B sono rappresentativi, ciascuno, della coerenza di una prima firma 202A con una corrispondente seconda firma 202B, ovvero di una prima firma 202A derivata a partire da una prima immagine 201A del flusso di prime immagini 201A e di una seconda firma 202B derivata da una corrispondente seconda immagine 201B del flusso di seconde immagini 201B.

A5. In caso di esito positivo di un segnale del flusso di primi segnali di verifica 204A e secondi segnali di verifica 204B, ovvero in caso di esito positivo della verifica di coerenza di una coppia, abilitazione, da parte del circuito *watch-dog* 205 conforme ai requisiti prescritti per i massimi livelli di

safety integrity per applicazioni *safety-critical* CENELEC EN 50128 ed EN 50129, ad una trasmissione, da parte del terminale di calcolo 2, a partire dal flusso di prime immagini 201A o dal flusso di seconde immagini 201B, di un flusso di immagini di uscita 206 destinato ad essere visualizzato.

A6. In caso di esito negativo di almeno un segnale tra i segnali del flusso di primi segnali di verifica 204A o del flusso di secondi segnali di verifica 204B, interruzione, da parte del circuito *watch-dog* 205, della trasmissione del flusso di immagini di uscita 206 da parte del terminale di calcolo 2.

In un esempio di realizzazione, il metodo prevede le ulteriori fasi di:

B0. Predisposizione di un terminale operatore COTS 3 e di un server di trasferimento 4, in particolare di un server di rete, il server di rete essendo connesso al terminale di calcolo 2 e al terminale operatore COTS 3, il server di rete provvedendo un *workspace* protetto, ovvero un ambiente in cui le comunicazioni tra il terminale di calcolo 2 e il terminale operatore COTS 3 avvengono in maniera sicura e protetta da intrusioni.

B1. Criptazione e compressione, da parte del terminale di calcolo 2, di ciascuna immagine del flusso di immagini di uscita 206.

B2. Trasmissione, da parte del terminale di calcolo 2, del flusso di immagini di uscita 206 criptato e trasmesso al server di trasferimento 4, ovvero al server di rete.

B3. Decriptazione e decompressione, da parte del server di rete, di ciascuna immagine del flusso di immagini di uscita 206 e aggiornamento di una pagina web contenente ciascuna immagine del flusso di immagini in di uscita 206.

B4. Alimentazione, ovvero trasmissione di ciascun aggiornamento della pagina web contenente ciascuna immagine del flusso di immagini di uscita 206 al terminale operatore COTS 3

B5. Visualizzazione, su uno schermo 300 del terminale operatore COTS 3, della pagina web aggiornata.

In un esempio di realizzazione, il metodo prevede le seguenti fasi:

C1. Generazione, da parte di un terminale operatore 3 di un segnale di

comando 304, attraverso una tastiera 302 e un mouse 303. Invio del segnale di comando 304, da parte del terminale operatore 3, al terminale di calcolo 2.

C2. Ricezione, da parte del terminale di calcolo 2, del segnale di comando 304 e generazione, in risposta al segnale di comando 304, di una *one-time password* 306 e di un segnale di richiesta 307 di un inserimento della *one-time password* 306 da parte di un operatore. Invio, da parte del terminale di calcolo 2, della *one-time password* 306, ad un dispositivo mobile personale 308, ad esempio uno smartphone, a disposizione di un operatore, oppure direttamente al terminale operatore 3. Invio, da parte del terminale di calcolo 2, del segnale di richiesta 307 di inserimento della *one-time password* 306, al terminale operatore 3.

C3. Restituzione, da parte del terminale operatore 3, della *one-time password* 306, in risposta al segnale di richiesta 307.

C4. Controllo, da parte del terminale di calcolo 2, che la *one-time password* 306 inviata dal terminale di calcolo 2 al dispositivo mobile personale 308 o al terminale operatore 3, e la *one-time password* restituita, dal terminale operatore 3 al terminale di calcolo 2 siano coerenti l'una con l'altra.

C5. In caso di esito positivo del controllo di coerenza, inoltro, da parte del terminale di calcolo 2, del segnale di controllo 304, alla piattaforma di controllo e comando 10.

In un esempio, il metodo include una fase di ricezione, al terminale di calcolo (2), del segnale di comando (304) generato e trasmesso da parte del terminale operatore COTS (3); il metodo comprende inoltre una fase di generazione e trasmissione, al terminale di calcolo (2), di un segnale di conferma del comando da parte di un operatore; il terminale di calcolo (2) riceve il segnale di conferma del comando e trasmette il segnale di comando (304), alla ricezione del segnale di conferma del comando.

IL MANDATARIO
Ing. Marco CONTI
(Albo iscr. n. 1280 BM)

RIVENDICAZIONI

1. Sistema (1) per rappresentare lo stato di un impianto ferroviario, comprendente:

- una piattaforma di controllo e comando (10), configurata per fornire un flusso di dati di ingresso (100) rappresentativi dello stato dell'impianto ferroviario;

- un terminale di calcolo (2), configurato per ricevere dalla piattaforma di controllo e comando (10) il flusso di dati di ingresso (100), il terminale di calcolo (2) includendo:

un primo processore (200A), programmato per generare, a partire dal flusso di dati di ingresso (100), un flusso di prime immagini (201A) e

un secondo processore (200B), programmato per generare, a partire dal flusso di dati di ingresso (100), un flusso di seconde immagini (201B),

in cui il primo processore (200A) e il secondo processore (200B) sono programmati per generare le rispettive immagini in un formato raw, e per convertire ciascuna immagine dal formato raw ad un predeterminato formato standard, eseguendo applicativi conformi ai requisiti prescritti per i massimi livelli di *safety integrity* per applicazioni *safety-critical* che non utilizzano librerie commerciali, e in particolare non utilizzano librerie grafiche commerciali,

in cui il terminale di calcolo (2) è configurato per

verificare che, per ciascuna coppia d'immagini formata da una prima immagine del flusso di prime immagini (201A) e una corrispondente seconda immagine del flusso di seconde immagini (201B), la prima e la seconda immagine siano coerenti l'una con l'altra, e

in risposta a detta verifica, generare, a partire dal flusso di prime (201A) o di seconde immagini (201B), un flusso d'immagini di uscita (206) destinato ad essere visualizzato da un terminale operatore (3) di tipo *commercial off-the-shelf* (COTS), di tipo fisso o mobile, connesso tramite rete aperta al terminale di calcolo (2).

2. Sistema (1) secondo la rivendicazione **1**, in cui il terminale di calcolo (2) include un canale di comunicazione bi-direzionale (203) tra il primo processore (200A) e il secondo processore (200B), il canale di comunicazione bi-direzionale (203) essendo configurato per condividere informazioni tra il primo processore (200A) e il secondo processore (200B), e in cui il primo processore (200A) e secondo processore (200B) sono programmati ciascuno per verificare la coerenza di ciascuna coppia di immagini e per generare un primo segnale di verifica (204A) e un secondo segnale di verifica (204B), rispettivamente, ciascun primo (204A) e secondo segnale di verifica (204B) essendo rappresentativo della coerenza della coppia d'immagini.

3. Sistema (1) secondo la rivendicazione 2, in cui il primo (200A) e il secondo processore (200B) sono programmati per derivare, a partire dalla prima immagine (201A) e dalla seconda immagine (201B), rispettivamente, una corrispondente prima (202A) e seconda firma (202B), e in cui le informazioni condivise tra il primo (200A) e il secondo processore (200B) includono la prima (202A) e la seconda firma (202B), per ciascuna coppia d'immagini, il primo (200A) e il secondo processore (200B) essendo programmati per verificare una coerenza tra la prima (202A) e la seconda firma (202B).

4. Sistema (1) secondo una qualsiasi delle rivendicazioni precedenti, in cui il terminale di calcolo (2) è provvisto di un sistema operativo in tempo reale conforme ai requisiti prescritti per i massimi livelli di *safety integrity* per applicazioni *safety-critical*, il terminale di calcolo (2) essendo configurato per svolgere, sotto la supervisione del sistema operativo in tempo reale (210), la generazione del flusso di prime immagini (201A) e del flusso di seconde immagini (201B) nel formato *raw*, la conversione di ciascuna immagine dal formato *raw* al predeterminato formato standard, la verifica della coerenza della coppia d'immagini e la generazione del flusso di immagini di uscita (206).

5. Sistema (1) secondo una delle rivendicazioni precedenti, comprendente,

oltre al terminale di calcolo (2), un server di trasferimento (4), il server di trasferimento (4) provvedendo un *workspace* protetto, conforme a requisiti di *security* previsti dalle normative europee ed applicabili al settore del presente trovato, in cui:

- il terminale di calcolo (2) è configurato per

criptare e comprimere ciascuna immagine di uscita del flusso di immagini di uscita (206),

trasmettere il flusso di immagini di uscita (206) al server di trasferimento (4),

- il server di trasferimento (4) è configurato per

decriptare e decomprimere ciascuna immagine del flusso di immagini di uscita (206) e

rendere disponibile ciascuna immagine del flusso di immagini di uscita (206) ad un terminale operatore (3) COTS, operativamente connesso al server di trasferimento (4), attraverso un collegamento di comunicazione, disponibile almeno per il tempo necessario a completare la sessione di lavoro.

6. Sistema (1) secondo una qualsiasi delle rivendicazioni dalla 1 alla 4, comprendente, oltre al terminale di calcolo (2), un server di trasferimento (4) in cui:

- il terminale di calcolo (2) è configurato per

criptare e comprimere ciascuna immagine di uscita del flusso di immagini di uscita (206),

trasmettere il flusso di immagini di uscita (206) al server di trasferimento (4),

- il server di trasferimento (4) è configurato per

rendere disponibile ciascuna immagine del flusso di immagini di uscita (206) al terminale operatore (3) COTS,

- il terminale operatore COTS (3) è configurato per

decriptare e decomprimere ciascuna immagine del flusso di immagini di uscita (206), il terminale operatore COTS (3) essendo operativamente

connesso al server di trasferimento (4), attraverso un collegamento di comunicazione, disponibile almeno per il tempo necessario a completare la sessione di lavoro.

7. Sistema (1) secondo una qualsiasi tra le rivendicazioni precedenti, in cui:

- il terminale di calcolo (2) è configurato per

ricevere un segnale di comando (304) dal terminale operatore di tipo COTS (3),

generare una *one-time password* (306) in risposta al segnale di comando (304) e un segnale di richiesta (307) per il terminale operatore (3), di inserimento della *one-time password* (306) da parte dell'operatore;

- il terminale operatore COTS (3) è configurato per

generare e trasmettere il segnale di comando (304) al terminale di calcolo (2),

ricevere la *one-time password* (306) e

restituire la *one-time password* (306) al terminale di calcolo (2) in risposta al segnale di richiesta (307), dal terminale di calcolo (2), di inserimento della *one-time password*;

il terminale di calcolo (2) essendo ulteriormente configurato per

verificare che la *one-time password* (306) generata dal terminale di calcolo (2) e la *one-time password* (306) restituita dal terminale operatore (3) COTS siano coerenti l'una con l'altra e

trasmettere il segnale di comando (304) alla piattaforma di controllo e comando (10) in conseguenza a detta verifica.

8. Sistema (1) secondo una qualsiasi tra le rivendicazioni precedenti, in cui almeno una delle seguenti condizioni è verificata:

- un canale di trasmissione di una *one-time password* (306) da e verso il terminale operatore (3) COTS è diverso dal canale di trasmissione utilizzato per la trasmissione di dati tra terminale di calcolo (2) e terminale operatore COTS (3);

- una trasmissione di tutti i dati, ovvero della *one-time password* (306) e dei dati, viene realizzata in un ambito di un *workspace* protetto fornito da un

server di trasferimento (4).

9. Sistema (1) secondo una qualsiasi delle rivendicazioni precedenti, in cui il terminale di calcolo (2) include un circuito *watch-dog* (205) conforme ai requisiti prescritti per i massimi livelli di *safety integrity* per applicazioni *safety-critical*, connesso al primo processore (200A) e al secondo processore (200B) e configurato per disabilitare il flusso di immagini di uscita (206), in risposta ad un esito negativo della verifica della coppia d'immagini o di una qualunque altra anomalia con potenziale impatto sulla *safety* del sistema.

10. Metodo per rappresentare lo stato di un impianto ferroviario, comprendente le seguenti fasi:

- predisposizione, da parte di una piattaforma di controllo e comando (10), di un flusso di dati di ingresso (100), rappresentativi dello stato dell'impianto ferroviario;
- ricezione, ad un terminale di calcolo (2), del flusso di dati di ingresso (100);
- generazione, da parte del terminale di calcolo (2) a partire dal flusso di dati di ingresso (100), di un flusso di prime immagini (201A) in formato *raw*;
- generazione, da parte del terminale di calcolo (2) a partire dal flusso di dati di ingresso (100), di un flusso di seconde immagini (201B) in formato *raw*;
- conversione, da parte del terminale di calcolo (2), delle prime immagini del flusso di prime immagini (201A) e delle seconde immagini del flusso di seconde immagini (201B) dal formato *raw* ad un formato standard,
- verifica, da parte del terminale di calcolo (2), per ciascuna coppia d'immagini formata da una prima immagine del flusso di prime immagini (201A) e da una corrispondente seconda immagine del flusso di seconde immagini (201B), che la prima e la seconda immagine siano coerenti l'una con l'altra, e
- in funzione di detta verifica, generazione, da parte del terminale di calcolo (2) a partire dal flusso di prime (201A) o seconde immagini (201B), di un flusso di immagini di uscita (206) destinato ad essere visualizzato da un terminale operatore (3) di tipo COTS connesso tramite rete aperta al

terminale di calcolo (2).

11. Metodo secondo la rivendicazione 10 in cui la fase di generazione del flusso di prime immagini (201A) e di conversione delle immagini del flusso di prime immagini (201A) al formato standard è eseguita da un primo processore (200A) e in cui la fase di generazione del flusso di seconde immagini (201B) e di conversione delle immagini del flusso di seconde immagini (201B) al formato standard è eseguita da un secondo processore (200B), il primo processore (200A) e il secondo processore (200B) essendo processori distinti del terminale di calcolo (2) e tali processori eseguendo applicativi conformi ai requisiti prescritti per i massimi livelli di *safety integrity* per applicazioni *safety-critical*, senza la necessità di utilizzare librerie grafiche commerciali per la generazione delle immagini.

12. Metodo secondo la rivendicazione 11, in cui il terminale di calcolo (2) include un canale di comunicazione bi-direzionale (203) tra il primo processore (200A) e il secondo processore (200B), il metodo comprendendo le seguenti fasi:

- condivisione di informazioni tra il primo processore (200A) e il secondo processore (200B), attraverso il canale bi-direzionale (203),
- verifica, da parte del primo processore (200A) e del secondo processore (200B), della coerenza di una rispettiva coppia d'immagini,
- generazione, da parte del primo processore (200A) e del secondo processore (200B), di un primo segnale di verifica (204A) e di un secondo segnale di verifica (204B), rispettivamente, ciascun segnale di verifica del primo (204A) e del secondo segnale (204B) di verifica essendo rappresentativo di una coerenza della coppia d'immagini.

13. Metodo secondo la rivendicazione 12, comprendente ulteriormente una fase di

- derivazione, da parte del primo (200A) e del secondo processore (200B), a partire dalla prima immagine (201A) e dalla seconda immagine (201B), rispettivamente, di una corrispondente prima firma (202A) e seconda firma (202B), in cui la fase di condivisione di informazioni tra il primo (200A) e il

secondo processore (200B) include la condivisione della prima (202A) e della seconda firma (202B), per ciascuna coppia d'immagini e in cui la fase di verifica della coerenza tra la prima immagine (201A) e la seconda immagine (201B) include una verifica tra la prima (202A) e la seconda firma (202B).

14. Metodo secondo una qualsiasi delle rivendicazioni dalla 10 alla 13, comprendente una fase di interruzione, da parte di un circuito *watch-dog* (205) conforme ai requisiti prescritti per i massimi livelli di *safety integrity* per applicazioni *safety-critical*, del flusso di immagini di uscita (206), in risposta ad un esito negativo della verifica o di qualunque altra anomalia con potenziale impatto sulla *safety* del sistema.

15. Metodo secondo una qualsiasi delle rivendicazioni dalla 10 alla 14, comprendente le seguenti fasi:

- predisposizione di un server di trasferimento (4), il server di trasferimento (4) provvedendo un *workspace* protetto conforme a requisiti di *security* previsti dalle normative europee ed applicabili al settore del presente trovato,
- criptazione e compressione, da parte del terminale di calcolo (2), delle immagini di uscita del flusso di immagini di uscita (206) e trasmissione, da parte del terminale di calcolo (2), del flusso di immagini di uscita (206) al server di trasferimento (4),
- decriptazione e decompressione, da parte del server di trasferimento (4), delle immagini di uscita del flusso di immagini di uscita (206),
- predisposizione di un terminale operatore (3) di tipo COTS connesso al terminale di calcolo (2) tramite una rete aperta, il terminale operatore (3) di tipo COTS essendo operativamente connesso al server di trasferimento (4), attraverso un collegamento di comunicazione, disponibile almeno per il tempo necessario a completare la sessione di lavoro,
- trasmissione al terminale operatore (3) di tipo COTS, da parte del server di trasferimento (4), del flusso di immagini di uscita (206),
- visualizzazione, da parte del terminale operatore (3) di tipo COTS, del

flusso di immagini di uscita (206).

16. Metodo secondo una qualsiasi delle rivendicazioni dalla 10 alla 14, comprendente le seguenti fasi:

- predisposizione di un server di trasferimento (4), il server di trasferimento (4) provvedendo un *workspace* protetto,
- criptazione e compressione, da parte del terminale di calcolo (2), delle immagini di uscita del flusso di immagini di uscita (206) e trasmissione, da parte del terminale di calcolo (2), del flusso di immagini di uscita (206) al server di trasferimento (4),
- predisposizione di un terminale operatore (3) di tipo COTS connesso al terminale di calcolo (2) tramite una rete aperta, il terminale operatore (3) di tipo COTS essendo operativamente connesso al server di trasferimento (4), attraverso un collegamento di comunicazione, disponibile almeno per il tempo necessario a completare la sessione di lavoro,
- trasmissione al terminale operatore (3) di tipo COTS, da parte del server di trasferimento (4), del flusso di immagini di uscita (206);
- decriptazione e decompressione, da parte del terminale operatore (3) di tipo COTS, delle immagini di uscita del flusso di immagini di uscita (206),
- visualizzazione, da parte del terminale operatore (3) di tipo COTS, del flusso di immagini di uscita (206).

17. Metodo secondo una qualsiasi delle rivendicazioni dalla 10 alla 16, comprendente le seguenti fasi:

- da parte del terminale di calcolo (2),

ricezione di un segnale di comando (304) da parte del terminale operatore (3) di tipo COTS,

generazione di una *one-time password* (306) in risposta al segnale di comando (304) e di un segnale di richiesta (307) di un inserimento della *one-time password* per il terminale operatore (3) di tipo COTS;

- da parte del terminale operatore (3) di tipo COTS,

generazione e trasmissione del segnale di comando (304) al terminale di calcolo (2),

ricezione della *one-time password* (306) e

restituzione della *one-time password* (306) al terminale di calcolo (2) in risposta al segnale di richiesta (307) di inserimento dal terminale di calcolo (2),

il metodo ulteriormente comprendendo le fasi, da parte del terminale di calcolo (2), di

verifica che la *one-time password* (306) generata dal terminale di calcolo (2) e la *one-time password* (306) restituita dal terminale operatore (3) di tipo COTS siano coerenti l'una con l'altra e

trasmissione del segnale di comando (304) alla piattaforma di controllo e comando (10), in risposta a detta verifica.

Bologna, 24.02.2022

IL MANDATARIO
Ing. Marco CONTI
(Albo iscr. n. 1280 BM)

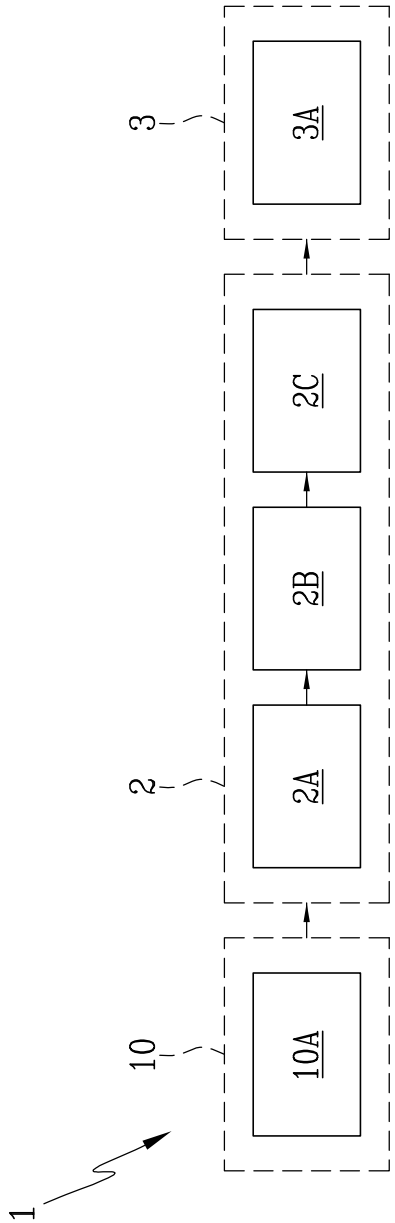

Fig.1

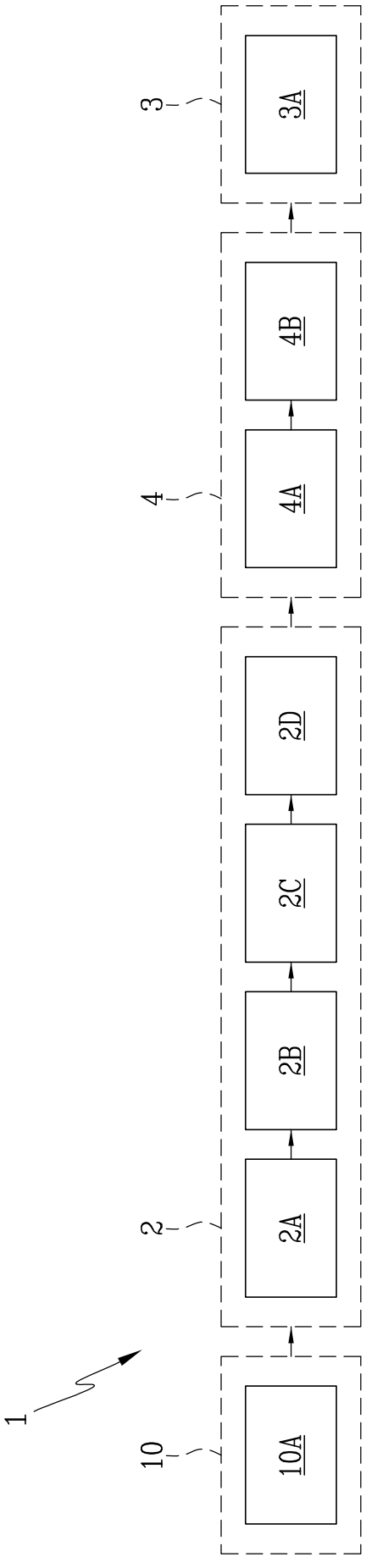

Fig.2

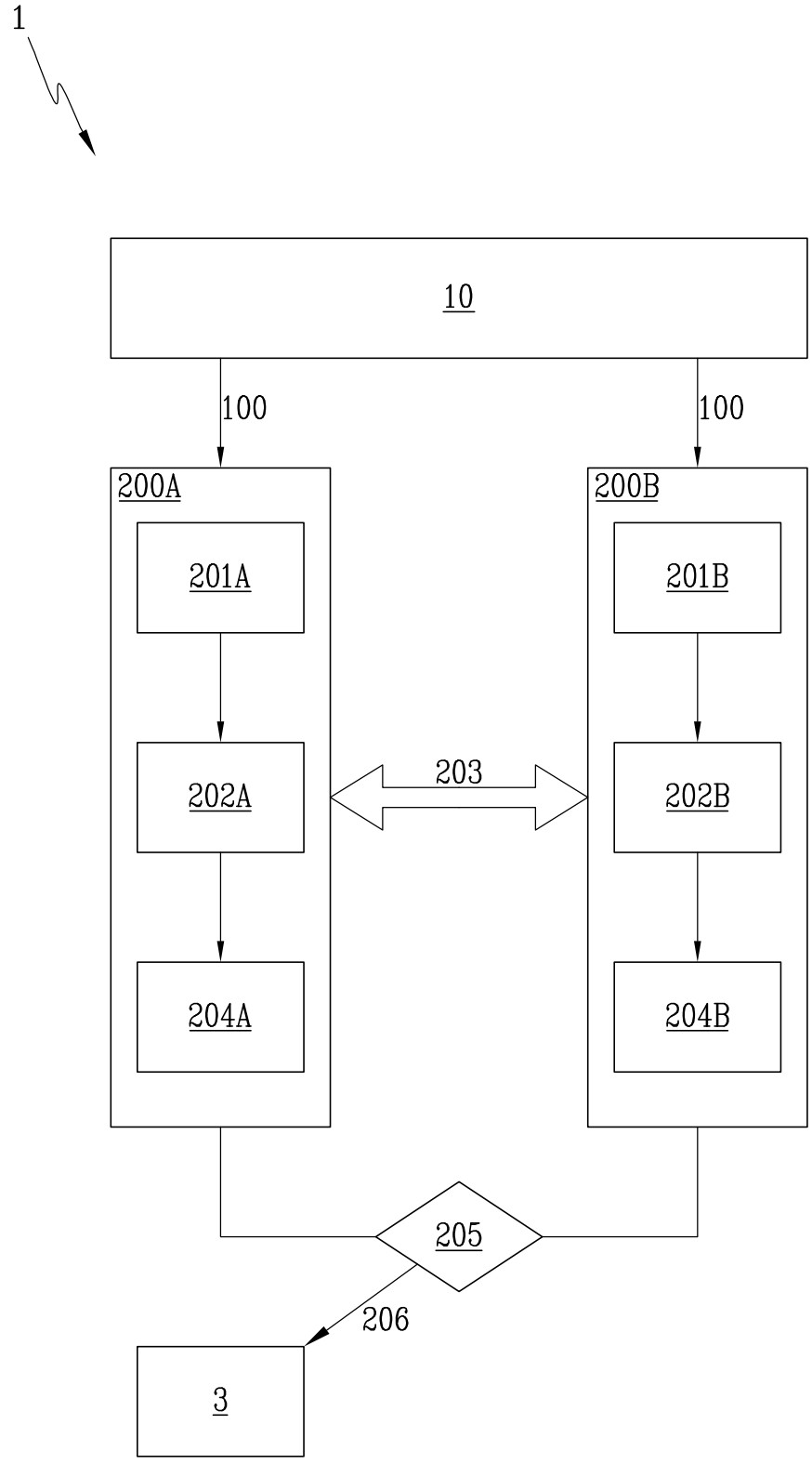
1
10
100
100
200A
200B
201A
201B
202A
203
202B
204A
204B
205
206
3

Fig.3

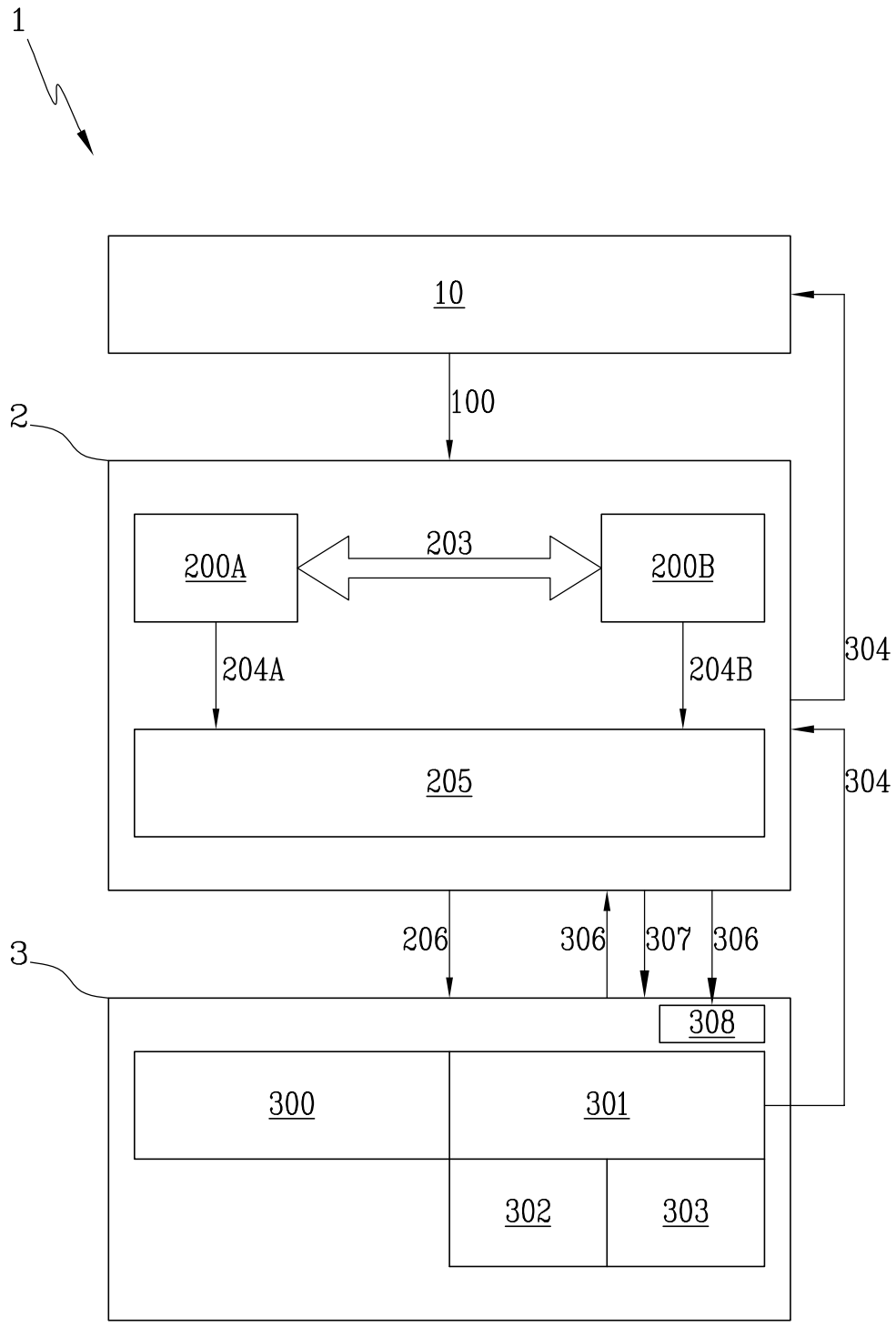
1
10
100
2
200A
203
200B
204A
204B
304
205
304
206
306
307
306
3
308
300
301
302
303

Fig.4

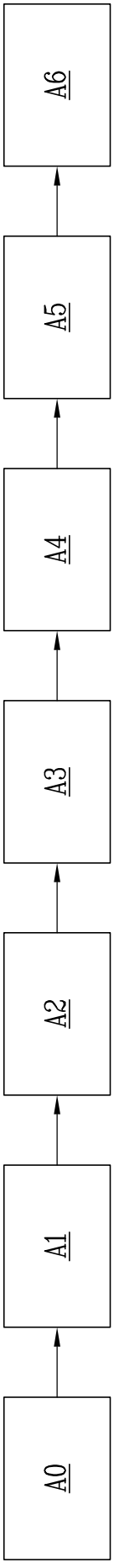

Fig.5

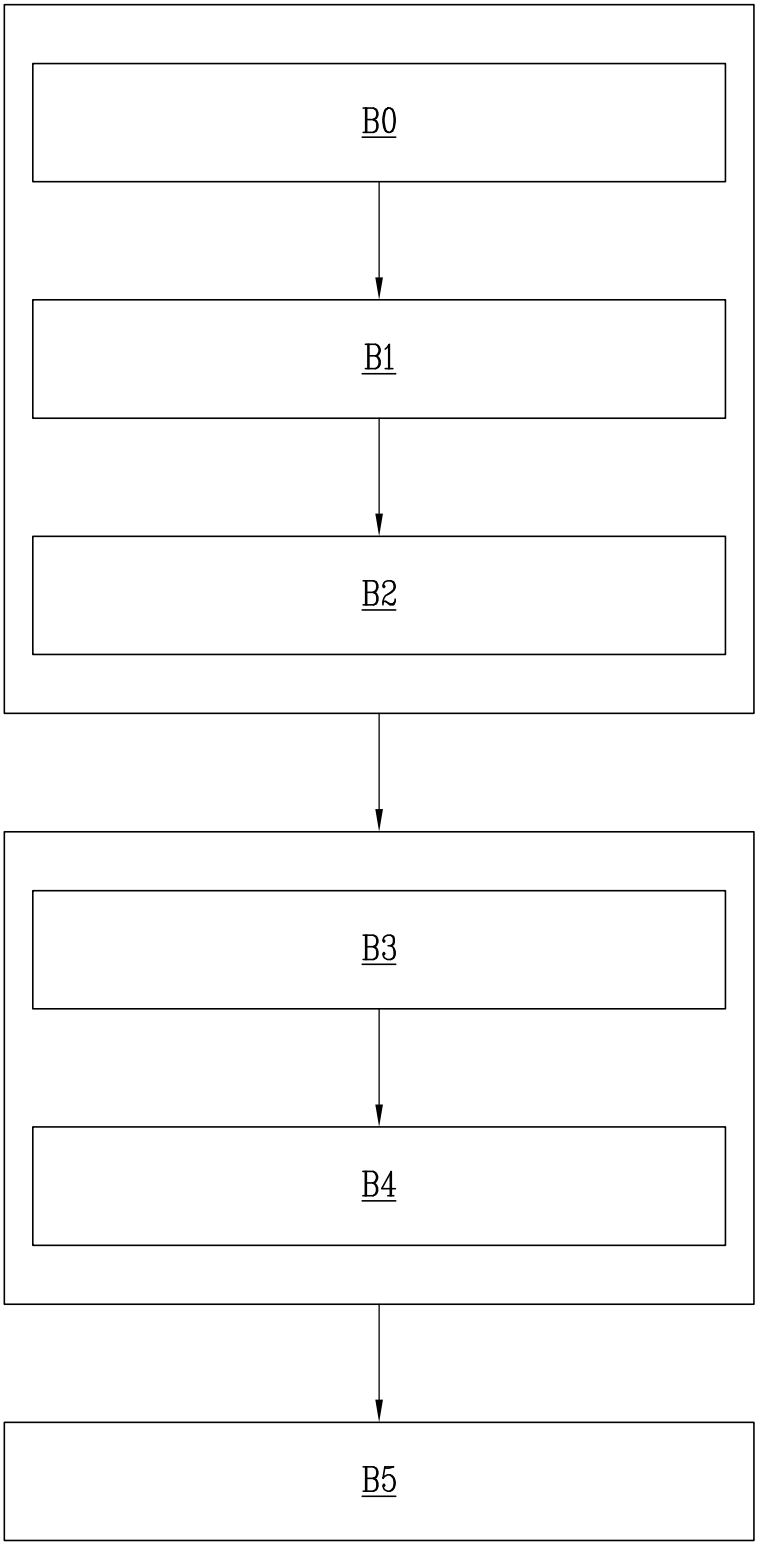

Fig.6

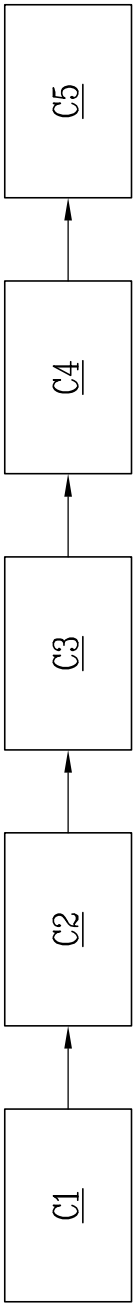

Fig.7