Informazioni identificative della domanda di Brevetto per invenzione industriale presentata il 31/12/2018

Dati aggiornati al 20/06/2022

Numero domanda: 102018000021550
Data presentanzione: 31/12/2018
Data deposito: 31/12/2018
Tipologia domanda: Brevetto per invenzione industriale
Tipo deposito: DEPOSITO ON LINE
Tipo domanda: Ordinaria
Tipo registrazione: Primo Deposito
Stato domanda: Concessa
Data concessione: 26/03/2021
Numero domanda precedente formato:
Numero concessione: 102018000021550
Titolo: PROCEDIMENTO DI PROTEZIONE DA ATTACCHI INFORMATICI AL VEICOLO E CORRISPONDENTE DISPOSITIVO
Anticipata accessibilità: NO

Classi

Sezione	Classe	Sottoclasse	Gruppo	Sottogruppo	Note
H	04	L	1		Classificazione inserita dall'EPO
G	06	F	21	55	Classificazione inserita dall'EPO
G	06	F	21	60	Classificazione inserita dall'EPO

Inventori

Cognome e nome
BALDANZI Luca
FANUCCI Luca
CROCETTI Luca
NESCI Walter
ROSADINI Christian

Titolari

Denominazione/cognome e nome	Tipo società	Partita I.V.A./C.F.	Diritti %	CAP	Città	Provincia	Nazione
UNIVERSITA' DI PISA	le universita'	00286820501	50	56126	Pisa	Pisa	Italia
MAGNETI MARELLI S.P.A.	societa' per azioni	08082990014	50	20011	Corbetta	Milano	Italia

Mandatari

Cognome e nome (codice)
Buzzi Franco (259)
Gallarotti Franco (726)
Crovini Giorgio (857)
Bosotti Luciano (260)
Cesa Roberta (1651)
Notaro Giancarlo (258)
De Bonis Paolo (1513)
Frontoni Stefano (1309)
Freyria Fava Cristina (1123)
Marchitelli Mauro (507)
Meindl Tassilo Bertram (1427)

Domicilio elettivo

Nominativo	Via	Numero civico	Città	CAP	Provincia	Nazione	E-mail	PEC
Buzzi, Notaro & Antonielli d'Oulx S.p.A.	Corso Vittorio Emanuele II, 6		Torino	10123	Torino			brevetti@pec.bnaturin.eu

Studio

Nominativo: Buzzi, Notaro & Antonielli d'Oulx S.p.A.
Via: Corso Vittorio Emanuele II, 6
Numero civico:
Città: Torino
CAP: 10123
Provincia: Torino

Istanze

Numero	Data deposito	Descrizione	Esito	Data Esito
782020000164518	29/09/2020	Risposta a Rapporto di Ricerca		
812019000021061	19/02/2019	Scioglimento Riserve		

Pagamenti

Data	Importo	Tipo	Identificativo	Causale
31/12/2018	95,00	Modello F24	Deposito Pagamento Deposito, Annualita, Altri Tributi	

Ministero dello Sviluppo Economico

Ricevuta di presentazione

per

Brevetto per invenzione industriale

Domanda numero: 102018000021550

Data di presentazione: 31/12/2018

DATI IDENTIFICATIVI DEL DEPOSITO

Ruolo	Mandatario
Depositante	Giorgio Crovini
Data di compilazione	31/12/2018
Riferimento depositante	BIT21850-GC/li
Titolo	"Procedimento di protezione da attacchi informatici al veicolo e corrispondente dispositivo"
Carattere domanda	Ordinaria
Esenzione	NO
Accessibilità al pubblico	NO
Numero rivendicazioni	11
Autorità depositaria	

PRIVACY

Autorizzo il trattamento dei dati personali, inseriti all'interno del deposito, ai sensi del GDPR (Regolamento UE 2016/679) e del Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali"

RICHIEDENTE/I

Natura giuridica	Persona giuridica
Denominazione	MAGNETI MARELLI S.P.A.
Partita IVA	08082990014
Tipo Società	societa' per azioni
Nazione sede legale	Italia
Comune sede legale	Corbetta (MI)
Indirizzo	viale Aldo Borletti
Civico	61/63

CAP	20011
Telefono	
Fax	
Email	
Pec	brevetti@pec.bnaturin.eu
Quota percentuale	50.0%

Natura giuridica	Persona giuridica
Denominazione	UNIVERSITA' DI PISA
Partita IVA	00286820501
Tipo Società	le universita'
Nazione sede legale	Italia
Comune sede legale	Pisa (PI)
Indirizzo	Lungarno Antonio Pacinotti
Civico	43
CAP	56126
Telefono	
Fax	
Email	
Pec	brevetti@pec.bnaturin.eu
Quota percentuale	50.0%

DOMICILIO ELETTIVO

Cognome/R.sociale	Buzzi, Notaro & Antonielli d'Oulx S.r.l.
Indirizzo	Corso Vittorio Emanuele II, 6
Cap	10123
Nazione	Italia
Comune	Torino (TO)
Telefono	011 - 8392911
Fax	011 - 8392929
Email\PEC	brevetti@pec.bnaturin.eu

MANDATARI/RAPPRESENTANTI

Cognome	Nome
Bosotti	Luciano
Buzzi	Franco
Cesa	Roberta
De Bonis	Paolo
Freyria Fava	Cristina
Frontoni	Stefano
Gallarotti	Franco
Marchitelli	Mauro
Meindl	Tassilo Bertram
Notaro	Giancarlo
Crovini	Giorgio

INVENTORI

Cognome	Nome	Nazione residenza
ROSADINI	Christian	Italia
NESCI	Walter	Italia
BALDANZI	Luca	Italia
CROCETTI	Luca	Italia
FANUCCI	Luca	Italia

CLASSIFICAZIONI

Sezione	Classe	Sottoclasse	Gruppo	Sottogruppo
H	04	L	29	06

NUMERO DOMANDE COLLEGATE

DOCUMENTAZIONE ALLEGATA

Tipo documento	Riserva	Documento
Rivendicazioni	NO	bit21850 Rivendicazioni.pdf.p7m hash: 920d0657f079bddf5f4d8530344e253c
Descrizione in italiano*	NO	bit21850 Descrizione.pdf.p7m hash: bcaee6f482b18793fcfb42354ca299c1
Disegni	NO	bit21850 Disegni.pdf.p7m hash: b4e7236156e0e0ce675883a173a5fbfc
Riassunto	NO	bit21850 Riassunto.pdf.p7m hash: d7889614d5a42821af4e6a15edd5e554
Rivendicazioni in inglese	SI	hash:
Lettera di Incarico	SI	hash:

PAGAMENTI

Tipo	Identificativo	Data
Bollo	01170362637110	05/07/2018

DOVUTO

Gli importi indicati non tengono conto delle eventuali esenzioni applicabili

Importo Tasse:	€ 95,00
Importo Imposta Bollo:	€ 20,00

NOTE

RIASSUNTO

Viene descritto un procedimento di protezione da attacchi informatici in una rete di comunicazione CAN (Controller Area Network) (20) di un veicolo comprendente un bus CAN (10) e una pluralità di nodi (11) associati a detto bus CAN (10) in rapporto di scambio di segnale e associati almeno in parte a unità di controllo di funzioni del veicolo,

comprendente le operazioni di

analizzare il contenuto di messaggi CAN (M) in transito fra nodi di detta pluralità di nodi (11) per identificare messaggi CAN non leciti (MF),

bloccare (B1, B2) detti messaggi non leciti (MF), detta operazione di bloccare (B1, B2) comprendendo di rendere non validi (F1, F2) detti messaggi non leciti (MF) rispetto a una verifica di integrità eseguita da un controllore CAN (13) di detti nodi (11), inserendo (F1) una sequenza di bit (NV) di corruzione riconosciuta come un errore da detto controllore CAN (13), ottenendo un messaggio corrotto (MF'). Secondo la soluzione qui descritta è previsto di inserire (F1) detta sequenza di bit (NV) di corruzione in un campo di controllo integrità (S5), in particolare un campo CRC, del messaggio CAN non lecito (MF) a un tempo di bit (bt_{j-5}) il cui valore è tale da allineare temporalmente un campo separatore (ITM) del messaggio non lecito con un corrispondente campo separatore di un messaggio d'errore (EM) generato da un nodo della rete (20) che riceve detto messaggio non lecito (MF) comprendente detta sequenza di corruzione (NV). Al fine di garantire l'allineamento dei campi separatore (ITM) del messaggio non lecito (MF) e il messaggio d'errore (EM), la

soluzione qui descritta prevede anche un'operazione di oscuramento (F2) atta a mascherare l'invio del/dei messaggio/i di errore (EM) e ad emulare la corretta ricezione (OR) del/dei messaggio/i non lecito/i.

(Figura 6)

DESCRIZIONE dell'invenzione industriale dal titolo:
"Procedimento di protezione da attacchi informatici al veicolo e corrispondente dispositivo"
di: Magneti Marelli S.p.A., nazionalità italiana, viale Aldo Borletti 61/63, 20011 Corbetta MI e Università di Pisa, Lungarno Antonio Pacinotti 43, 56126 Pisa PI.
Inventori designati: Christian ROSADINI, Walter NESCI, Luca BALDANZI, Luca CROCETTI, Luca FANUCCI
Depositata il: 31 dicembre 2018

***

TESTO DELLA DESCRIZIONE

La presente invenzione riguarda tecniche di protezione da attacchi informatici in una rete di comunicazione CAN (Controller Area Network) di un veicolo comprendente un bus CAN e una pluralità di nodi associati a detto bus CAN in rapporto di scambio di segnale e associati almeno in parte a unità di controllo di funzioni del veicolo,

comprendente le operazioni di

analizzare il contenuto di messaggi CAN in transito fra nodi di detta pluralità di nodi per identificare messaggi CAN non leciti,

bloccare detti messaggi non leciti,

detta operazione di bloccare comprendendo di rendere non validi detti messaggi non leciti rispetto a una verifica di integrità eseguita da un controllore CAN di detti nodi, inserendo una sequenza di bit di corruzione riconosciuta come un errore da detto controllore CAN, in particolare sostituendo parte della sequenza originale di bit con una di corruzione, ottenendo un messaggio corrotto.

Il bus CAN, adottato come BUS di comunicazione negli autoveicoli, è un mezzo di comunicazione di tipo seriale e multi-master, in cui ogni master, detto anche nodo connesso

al bus è in grado di inviare, ricevere e risolvere i conflitti di accesso contemporaneo in invio da parte di più nodi.

Un nodo 11 in grado di comunicare su bus CAN 10 comprende in generale, come mostrato in figura 1a:

- un ricetrasmettitore CAN, o CAN Transceiver, 12, associato attraverso a una linea di trasmissione TT e una linea di ricezione TR al CAN bus 10 e configurato per gestire i livelli elettrici propri del bus CAN (livello Fisico del modello OSI);
- un controllore CAN, o CAN Controller, 13, che è connesso attraverso rispettive linee di trasmissione CT e ricezione CR al ricetrasmettitore CAN 12, e configurato per gestire i livelli logici e la serializzazione del bus CAN 10 (livello Data link del modello OSI);
- un microcontrollore 14, che contiene la logica di invio e ricezione dei messaggi (gestione dei livelli OSI superiori al livello Data link).

In figura 1A è riportata una delle possibili soluzioni di implementazione che prevede che il controllore CAN 13 e il microcontrollore 14 siano posti in uno stesso System-on-Chip 15, mentre il ricetrasmettitore CAN è su un chip separato.

E’ noto installare un dispositivo di protezione 16 da attacchi informatici tra il controllore CAN 13 e il ricetrasmettitore CAN 12, come mostrato in Figura 1. Il dispositivo di protezione 16 elabora, in particolare analizza, i messaggi in transito tra il controllore CAN 13 e il ricetrasmettitore CAN 12 individuando i messaggi non leciti, o malevoli, e attua delle operazioni di bloccaggio dell’iniezione di tali messaggi malevoli su bus CAN in

differenti casi d'uso, che sono descritti nelle Figure 2, 3, 4 e 5.

In particolare, in figura 1B il dispositivo di protezione 16 riceve messaggi CAN sulla linea di trasmissione CT dal controllore CAN 13 al dispositivo di protezione 16, li analizza e li filtra, tramite le summenzionate operazioni di bloccaggio, sicché la linea fra dispositivo di protezione 16 e ricetrasmettitore CAN 12 è una linea di trasmissione filtrata DT su cui transitano i messaggi CAN elaborati dal dispositivo di protezione 16. Viceversa i messaggi CAN arrivano dal ricetrasmettitore 12 al dispositivo di protezione sulla linea di ricezione CR, che connette tali moduli, e sono elaborati al dispositivo di protezione 16 e trasmessi su una linea di ricezione filtrata DR al controllore CAN 12 dal dispositivo di protezione 16.

In particolare in Figura 2, è mostrato un caso in cui data una rete veicolare 20 che comprende una pluralità di nodi 11_1….11_n, rappresentativi ad esempi di centraline veicolari, quali ECU (Electronic Control Unit), ad esempio Engine Control Unit, ma anche centraline per l'illuminazione, il condizionamento, controllo trasmissione, ABS, controllo sospensioni, e altri moduli a processore dedicati altri servizi veicolari. In tale pluralità di nodi 11_1…11_n il nodo 11_1 è un nodo protetto, equipaggiato di dispositivo di protezione 16, ed è raffigurato il caso in cui tale nodo 11_1 protetto è malevolo e inietta messaggi CAN, o CAN frame, malevoli, cioè non leciti, MF verso la rete veicolare 20. Tale caso d'uso è quello in cui ad esempio il microcontrollore 14 è stato violato per mezzo di altri canali di comunicazione, come ad esempio un canale wireless, come può accadere per

nodi corrispondenti a unità di Infotainment/Telematics. In questo caso la presenza del dispositivo di protezione 16 evita che tali messaggi MF raggiungano la rete veicolare 20, ossia gli altri nodi non protetti 11_2….11_n.

In Figura 3 è mostrato il caso in cui i messaggi CAN malevoli MF sono iniettati dalla rete veicolare 20, ossia da uno dei nodi privi di dispositivo di protezione, ossia nodi non protetti, 11_2….11_n, in particolare il nodo 11_2. Tale figura rappresenta il caso d'uso in cui un nodo qualunque della rete veicolare 20 è stato violato. In questo caso la presenza del dispositivo di protezione 16 evita che i messaggi non pertinenti al rispettivo nodo CAN protetto 11_1 su cui è installato possano essere elaborati dal microcontrollore 14.

In Figura 4 è mostrato il caso in cui il dispositivo di protezione 16 è impiegato all'interno di un CAN gateway 18. Tale configurazione permette di isolare due reti CAN distinte 20A e 20B, con rispettivi nodi $11A_1$…$11A_n$ e $11B_1$…$11B_n$, in generale non protetti, di garantire il filtraggio dei frame CAN in transito da e tra una rete e l'altro. Nel caso specifico di figura 4, il dispositivo di protezione 16 blocca i messaggi non leciti MF trasmessi dalla rete 20A e ne impedisce la diffusione sulla rete 20B. E' chiaro che il dispositivo di protezione 16 può anche bloccare un messaggio CAN non lecito MF trasmesso da un nodo della rete 20B verso la rete 20A attraverso il gateway 18.

La domanda di brevetto statunitense US2015/191136 A1 descrive un dispositivo di protezione che opera in CAN bus di autoveicoli che prevede di bloccare messaggi in transito i cui parametri verificano criteri di messaggio non lecito. Il blocco è operato rendendo non validi rispetto a una

verifica di validità eseguita dal controllore CAN, ossia corrompendo, i messaggi non leciti durante la loro trasmissione fra il ricetrasmettitore CAN e il controllore CAN, inserendo una sequenza di bit riconosciuta come un errore dal controllore CAN, in particolare bit di stuffing, o bit di riempimento, in particolare inserendo uno Stuff error mediante una sequenza che non rispetta la regola del bit stuffing previsto dal protocollo CAN che determina da parte del dal controllore CAN di ignorare tali messaggi non leciti e non propagare tali messaggi non leciti sulla rete CAN. Tuttavia, la manipolazione del numero di stuff bit può generare un disallineamento temporale tra il messaggio corrotto (inviato sul bus) ed il messaggio "Error-Frame" generato dal nodo CAN che riceve il messaggio corrotto.

La presente invenzione si prefigge lo scopo di ottenere un procedimento di monitoraggio che permetta di rendere non validi i messaggi non leciti, operando un corretto allineamento.

Secondo la presente invenzione, tale scopo viene raggiunto grazie ad un procedimento di protezione nonché a un corrispondente dispositivo di protezione aventi le caratteristiche richiamate in modo specifico nelle rivendicazioni che seguono.

L'invenzione verrà descritta con riferimento ai disegni annessi, forniti a puro titolo di esempio non limitativo, in cui:

- le Figure 1A e 1B, 2, 3, 4 sono già state descritte in precedenza;

- la Figura 5 rappresenta uno schema di principio del dispositivo di protezione implementante il procedimento qui descritto;

- la Figura 6 è un diagramma che rappresenta

schematicamente messaggi CAN elaborati dal dispositivo di protezione;

- le Figure 7A, 7B, 7C rappresentano schematicamente il dispositivo di protezione qui descritto in tre fasi di funzionamento del procedimento;

- la Figura 8 è un diagramma di flusso che rappresenta operazioni del procedimento qui descritto.

In Figura 5 è riportato uno schema a blocchi di principio di un dispositivo di protezione 26 secondo l'invenzione. Tale dispositivo di protezione 26 è mostrato disposto fra un controllore CAN 13 e un ricetrasmettitore CAN 12 in un nodo protetto di una rete CAN 10, come ad esempio nella configurazione di figura 3 del nodo 11_1. La soluzione qui descritta prescinde dalla versione di CAN su cui è applicata (CAN2.0 e CAN-FD, quindi) e per semplicità di esposizione viene descritto solo lo scenario relativo alla versione CAN2.0

Il dispositivo di protezione 26 comprende un modulo di firewall 261, che in generale riceve una sequenza di messaggi CAN M inviati sulla linea di ricezione CR e sulla linea di trasmissione CT e invia una sequenza filtrata di messaggi CAN sulle linee filtrate di ricezione DR e trasmissione DT. I messaggi M possono essere, come detto, messaggi non leciti MF. La sequenza filtrata, come meglio descritto nel seguito, può contenere i messaggi CAN M medesimi, può contenere messaggi corrotti MF' ottenuti dai messaggi non leciti MF oppure può applicare il blocco tramite corruzione (modalità B2 descritta nel seguito) in modo totale ai messaggi M leciti e non leciti MF.

Dunque, tale modulo di firewall 261 è configurato per:

- estrarre il contenuto informativo di un messaggio CAN M transitante sulle linee di trasmissione CT o

ricezione CR;

- operare l'analisi di tale contenuto informativo. Ciò ad esempio comprende confrontare valori di campi del messaggio CAN M transitante con un insieme di regole di firewall R memorizzate in un modulo di immagazzinamento regole 262 che rappresenta una base dati di regole, cui il modulo di firewall 261 ha accesso almeno in lettura;
- rendere non valido il messaggio CAN M in transito, qualora identificato in base al contenuto come messaggio CAN non lecito MF. Ciò avviene operandone la corruzione durante la trasmissione dal dispositivo di protezione 26 in accordo a modalità di blocco, ad esempio B1 e B2, meglio dettagliate nel seguito, nel caso in cui il messaggio M analizzato sia identificato come messaggio non lecito MF, mentre tale messaggio non lecito MF è ancora in transito sul bus CAN;

Come detto, il dispositivo di protezione 26 comprende inoltre una base dati di regole 262, che è la base dati che contiene regole R applicate dal firewall 261 ai messaggi CAN analizzati, cioè in transito, per identificare messaggi non leciti MF. I messaggi CAN M in transito, in arrivo dalla linea di trasmissione CT e dalla linea di ricezione CR, possono essere assoggettati a un medesimo insieme di regole R nel database di regole 262 oppure tale database di regole 262 può contenere due insiemi di regole applicati indipendentemente alla ricezione CR e alla trasmissione CT.

Il dispositivo di protezione 26 comprende inoltre un modulo di memorizzazione operazioni 263, ossia un'area di memoria dedicata per memorizzare un registro, o "log", di operazioni B svolte dal dispositivo di protezione 26 sul bus CAN 10. Il dispositivo di protezione 26 accede a tale

modulo 263 per scrivere tali operazioni B svolte dal dispositivo di protezione sul bus CAN 10. Tale registro B comprende statistiche relative all'attività del firewall 261, quali quantità di frame non leciti MF corrotti sulla linea di trasmissione CT, quantità di frame non leciti corrotti sulla linea di ricezione CR, etc …) e che possono essere consultate mediante un'interfaccia di configurazione 264 che può accedere in lettura al modulo di memorizzazione operazioni 263 come indicato in figura 5.

Il dispositivo di protezione 26 comprende poi, come detto, una interfaccia di configurazione 264 per definire le regole R di filtraggio applicate dal firewall 261 e memorizzate nel modulo 262. In particolare tale interfaccia di configurazione può ricevere una configurazione di filtraggio, cioè le regole R, del dispositivo di protezione 26 da un'interfaccia di comunicazione esterna non mostrata in figura. Tale interfaccia di configurazione 264 è in rapporto di scambio di dati con la base dati di regole 262, nella quale scrive ad esempio l'insieme di regole R per il filtraggio tramite firewall ed il modulo di memorizzazione operazioni 263, come detto ad esempio per leggere i dati del log delle operazioni del firewall 261.

Associato all'interfaccia di configurazione 264 è un modulo di autenticazione 265, che è configurato per verificare l'autenticità della configurazione di filtraggio ricevuta dall'interfaccia di comunicazione esterna, ad esempio tramite meccanismi di firma digitale e cifratura dei dati.

Il dispositivo di protezione 26 è in generale configurato per implementare un filtro che blocchi i messaggi CAN malevoli e non pertinenti, lasciando passare solamente i dati leciti

La distinzione tra messaggi leciti e illeciti può essere configurata in base alla destinazione d'uso del dispositivo di protezione 26 e definita attraverso i seguenti parametri distintivi C:

C1: identificativo messaggio CAN;

C2: lunghezza del messaggio CAN;

C3: tempi di trasmissione, ad esempio una frequenza nel caso di messaggio periodico;

C4: contenuto del messaggio. Tale parametro è impiegato solo per i messaggi di tipo diagnostico;

C5: stato del veicolo. Tale parametro è impiegato solo per i messaggi di tipo diagnostico;

C6: percentuale di utilizzo del bus nell'unità di tempo.

Il dispositivo di protezione 26 è configurato per applicare l'insieme delle regole R in generale ai messaggi non diagnostici e diagnostici, applicando in tale insieme ulteriori e specifiche regole di filtraggio nel caso in cui sia riconosciuto in transito un frame di tipo diagnostico

Il dispositivo di protezione 26 è inoltre configurato, in particolare tramite il modulo firewall 261, per operare due modalità di blocco del messaggio:

una modalità di blocco selettiva B1: vengono bloccati tutti e soli i messaggi CAN MF non leciti

una modalità di blocco totale B2: tutti i messaggi CAN vengono bloccati, sia leciti M che non leciti MF.

La modalità di blocco totale B2 è configurabile nei seguenti modi d'impiego:

primo modo d'impiego BC1, in la modalità di blocco totale B2 è abilitata o disabilitata,

secondo modo d'impiego BC2, in cui se la modalità di blocco totale B2 è abilitata, è possibile definire

nel dispositivo di protezione 26 il tipo di violazione e il numero di violazioni, per ognuno dei tipi di violazione specificati, raggiunto il quale la modalità di blocco totale B2 deve essere attivata, nonché il tempo per cui deve rimanere attiva. Nel secondo modo d'impiego B2 si definiscono quindi uno o più parametri di disattivazione in una lista comprendente tipo di violazione, numero di violazione, tempo di disattivazione;

La modalità di blocco totale B2 permette di disconnettere virtualmente un i-esimo nodo 11_i o una rete (es. 20B in figura 4) dal bus CAN 10 per un periodo di tempo arbitrario che, in base alla configurazione, può anche essere pressoché perpetuo, isolando quindi completamente il nodo 11_i o rete oppure ripristinando le capacità di comunicazione del nodo 11_i al termine del periodo di tempo impostato.

Il meccanismo mediante il quale il dispositivo di protezione 26 blocca un messaggio CAN non lecito implementa una modalità a zero-ritardo. Ciò rende vantaggioso l'utilizzo del dispositivo di protezione 26 in tutte le applicazioni in cui i ritardi di propagazione introdotti da elementi filtranti aggiuntivi, come appunto è il dispositivo di protezione 26, devono essere minimizzati.

Come detto, la modalità di filtraggio dei messaggi a zero-ritardo, implementata dal dispositivo di protezione 26, prevede di sfruttare i meccanismi di controllo integrità di per sé presenti nel bus CAN, rendendo non valido, cioè corrompendo, il messaggio CAN non lecito MF durante la trasmissione sul bus CAN, in modo tale che i nodi riceventi ignorino il suddetto messaggio non lecito MF già a livello digitale di controllore CAN 13, ossia il

livello Data link, ove viene effettuato il controllo di integrità del messaggio, senza andare a propagare il messaggio al microcontrollore 14 (e ai livelli superiori dello stack OSI). Pertanto, tale modalità a zero ritardo si contrappone a quella in cui l'elemento filtrante riceve-analizza-ritrasmette, come è tipico comportamento dei gateway, in quanto anche nella condizione ideale di tempi di analisi nullo, l'elemento filtrante deve comunque attendere che il messaggio termini prima di poterlo analizzare e, nel caso sia lecito e debba essere ritrasmesso, partecipare nuovamente alla fase di contesa e arbitraggio del bus (dopo la fase di analisi), introducendo un ritardo aggiuntivo pari ad almeno la durata della ritrasmissione del messaggio stesso. Inoltre, poiché è necessario che l'elemento filtrante vinca la contesa del bus CAN affinché possa procedere alla ritrasmissione del messaggio precedentemente analizzato, tale ritardo aggiuntivo può risultare essere significativamente più lungo, con un limite superiore, a causa delle caratteristiche del protocollo CAN, teoricamente infinito: caso di trasmissione di messaggi con priorità superiore da parte di altri nodi della rete.

La modalità a zero-ritardo implementata dal dispositivo di protezione 26 invece, permette di ispezionare un messaggio CAN in transito, cioè durante la trasmissione o la ricezione stessa da parte del nodo su cui è installato, e consente quindi:

- di agire prontamente corrompendo il messaggio non lecito prima ancora che la sua trasmissione o ricezione termini
- lasciar passare il messaggio inalterato se lecito, non impattando quindi il suo tempo di propagazione.

La procedura di filtraggio del frame CAN a zero ritardo, tramite la prima modalità di blocco selettivo B1 o seconda modalità di blocco totale B2, implementata dal dispositivo di protezione 26, comprende specificamente due operazioni che determinano che il tempo di propagazione del messaggio CAN non sia alterato e che il messaggio non lecito sia ritenuto, dal nodo malevolo, inviato con successo.

Una prima operazione è un'operazione F1 di blocco del messaggio in transito al dispositivo di protezione 26 tramite corruzione della sequenza di bit del messaggio CAN stesso.

Una seconda operazione è un'operazione F2 di oscuramento al nodo CAN malevolo che trasmette il messaggio CAN MF non lecito intercettato dal dispositivo di protezione 26 della corruzione di tale messaggio CAN non lecito da lui trasmesso, e quindi del suo conseguente bloccaggio da parte dei controlli d'integrità nei controllori CAN degli altri nodi CAN.

In conseguenza di tali modalità di blocco B1 o B2 tramite corruzione F1 e di oscuramento F2, il dispositivo di protezione 26 e il procedimento di protezione implementato da tale dispositivo 26 permettono di garantire la simultaneità tra la fine del transito del messaggio CAN non lecito, e corrotto tramite l'operazione F1 da parte del dispositivo di protezione 26, e la fine della trasmissione di un messaggio di errore in risposta a tale messaggio CAN non lecito corrotto, ossia come conseguenza derivante dalla rilevazione della condizione di errore introdotta dal dispositivo di protezione 26 nel messaggio CAN malevolo, al fine di corromperlo, da parte del/dei nodo/nodi CAN ricevente/i, $11_1 \ldots 11_n$, diversi dal nodo che comprende il

dispositivo di protezione 26 che applica l'operazione di blocco F1 al messaggio non lecito MF e diversi dal nodo CAN che inietta il messaggio malevolo MF.

Tale simultaneità rappresenta un aspetto fondamentale al fine di impedire l'innesco di sovrapposizioni non allineate di invio di messaggi che porterebbero a continue corruzioni dei dati sul bus CAN 10, con overhead sulla occupazione del bus, e, da ultimo, ad una interruzione della comunicazione.

Il procedimento di protezione implementato dal dispositivo di protezione tramite le operazioni di corruzione F1 e oscuramento F2 sfrutta la particolare struttura dei messaggi di tipo Dato ed Errore del protocollo CAN; in particolare il messaggio di tipo Dato è strutturato con sezioni S di bit contigue elencate di seguito nella tabella 1:

	Sezione S [dimensione in bit]	Contenuto sezione S
S1	SOF [1 bit]	inizio messaggio CAN
S2	Arbitration Field [12/32 bit]	contiene identificativo messaggio
S3	Control Field [6 bit]	contiene l'informazione della lunghezza dei dati trasmessi
S4	Data Field [0÷64 bit]	sezione dati (contenuto informativo del messaggio)
S5	CRC Field [16 bit]	codice per controllo integrità

		(con campo di delimiter)
S6	ACK Field [2 bit]	per conferma ricezione corretta da parte degli altri nodi (con campo di delimiter)
S7	EoF [7 bit]	zona di bit recessivi necessaria per segnalare la fine messaggio
S8	ITM [3 bit]	zona di bit recessivi che funge da separatore tra messaggi

Tabella 1

La struttura delle sezioni S del messaggio di tipo Dato è naturalmente di per sé nota, nello standard del bus CAN.

I messaggi di tipo Errore comprendono messaggi di tipo Attivo e Passivo strutturati come in Tabella 2 per l'Errore Attivo:

	Sezione S [dimensione in bit]	Contenuto sezione S
SE1	Active Error Flag[6 bit]	bit dominanti
SE2	Error delimiter[8 bit]	Campo che segnala la fine del messaggio di errore
SE3	ITM [3 bit]	zona di bit recessivi che funge da separatore

		tra messaggi

Tabella 2

mentre sono strutturati come in Tabella 3 per l'Errore Passivo:

	Sezione S [dimensione in bit]	Contenuto sezione S
SP1	Passive Error Flag[6 bit]	bit recessivi
SP2	Error delimiter[8 bit]	Campo che segnala la fine del messaggio di errore
SP3	ITM [3 bit]	zona di bit recessivi che funge da separatore tra messaggi

Tabella 3

In Figura 6, a titolo di esempio, viene mostrato un caso riferito all'Errore Attivo. Con MF è indicato il messaggio CAN non lecito in trasmissione, mentre con MF' è indicato il messaggio corrotto contenente in coda un messaggio d'errore EM, un messaggio CAN di tipo Errore in Risposta, da uno dei nodi riceventi, dopo che il controllo integrità del suo controllore CAN rileva la corruzione.

Con bt è indicato inoltre un'asse del tempo di bit e con NV un segnale scritto dal dispositivo di protezione 26 nel messaggio CAN non lecito MF. Con S_i è indicato il segnale interno generato dal dispositivo di protezione. In particolare il segnale S_i è il segnale DT nel dispositivo di protezione 26 nel caso di messaggio in trasmissione, o alternativamente è il segnale DR del dispositivo di protezione 26 nel caso di messaggio in ricezione.

Affinché sia garantita la simultaneità della fine della trasmissione del messaggio CAN non lecito MF, di tipo Data, corrotto dal dispositivo di protezione 26, e il

relativo messaggio EM di tipo Errore di risposta, emesso da parte di uno qualsiasi dei nodo riceventi 11, ovvero affinché i campi ITM (campo S8 per il messaggio non lecito MF e campo SE3 per il messaggio di errore EM) di tali messaggi siano allineati e sovrapposti, è necessario inserire una condizione di errore in un punto esatto, ossia ad uno specifico valore di bit time bt del messaggio non lecito MF. Ciò viene eseguito in particolare sostituendo parte della sequenza originale di bit con una di corruzione, ottenendo un messaggio corrotto.

Il punto esatto in cui effettuare l'inserimento della sequenza di corruzione di 6 bit consecutivi (NV) è univocamente determinato dal formato del pacchetto e dalle regole del protocollo CAN e richiede l'impiego di risorse/moduli logici dedicati al computo dello stesso e al computo della polarità dei bit che costituiscono detta sequenza di corruzione NV.

In particolare, per calcolare il punto di inizio della sequenza di 6 bit consecutivi all'interno del campo CRC e la polarità (dominante o recessiva) dei bit che la compongono, il dispositivo di protezione 26, in particolare il modulo di firewall 261, è dotato di uno o più moduli/elementi logici atti a o configurati per:

- calcolare dinamicamente (a runtime) il valore del campo CRC (Cyclic Redundancy Check) S5 al fine di prevedere il numero di stuff bit che saranno presenti all'interno del campo CRC;
- analizzare il contenuto del campo CRC ricostruito nel passo precedente tenendo conto anche dei bit che precedono il CRC, al fine di valutare il numero di stuff bit che saranno presenti nel campo CRC, ossia nel campo S5 del messaggio M, MF. Poiché il campo CRC

è data-dependent (e quindi varia a runtime così come i dati) anche il punto di inserzione esatto della sequenza di corruzione è determinato in modo dinamico.

Con riferimento alla figura 6, il punto esatto di inserzione nella sequenza di corruzione è l'istante bt_{j-5}, mentre l'istante in cui il nodo ricevente rileva la condizione di "Stuff error" (SPE) è l'istante bt_j. Con bt_{j-6} è indicato l'ultimo bit immediatamente precedente al primo bit della sequenza di corruzione, al fine di sottolineare che la sequenza di corruzione deve avere polarità opposta a tale bit.

In conseguenza di ciò:

- il nodo CAN 11 che riceve il messaggio MF corrotto risponde con un messaggio di errore EM (campi SE1, SE2, SE3 in quanto nell'esempio è illustrato un Errore Attivo, diversamente si impiegano i campi SP1, SP2, SP3 dell'Errore Passivo) a partire dal bit time bt_{j+1} immediatamente successivo a quello bt_j nel punto in cui si verifica la condizione di Stuff error SPE. Più specificamente, come mostrato nella figura 6, a partire dal bit time bt_{j+1} viene scritto il messaggio d'errore EM. Nel caso di più nodi riceventi, ciascun nodo ricevente 11_i trasmette un messaggio CAN EM di tipo Errore i cui frame d'errore sono esattamente sovrapposti a quelli di qualsiasi altro messaggio CAN EM di tipo Errore inviato da qualsiasi altro nodo ricevente;

- il termine del messaggio (o dei messaggi sovrapposti) di Errore, il campo SE3 ITM, che contiene una zona di bit recessivi, specificamente 3 bit, che funge da separatore tra messaggi è allineato temporalmente con il corrispondente campo ITM, S8, del messaggio non lecito MF, che è contemporaneamente ritrasmesso inalterato al nodo

malevolo mittente.

Anche a parità di lunghezza dei vari campi del frame di tipo Data di un messaggio CAN, la lunghezza del messaggio CAN può variare in base al loro contenuto, a causa della eventuale inserzione di bit di stuffing o bit di riempimento, pertanto il dispositivo di protezione 26 è configurato per calcolare dinamicamente, messaggio CAN per messaggio CAN, il punto di inserzione bt_{j-5} del campo CRC in cui è necessario inserire la sequenza NV di 6 bit consecutivi con la stessa polarità, nel caso in cui il frame MF debba essere corrotto. Il dispositivo di protezione 26 è configurato per calcolare dinamicamente, messaggio CAN per messaggio CAN, sia il punto di inserzione bt_{j-5} del campo CRC in cui è necessario inserire la sequenza NV di 6 bit consecutivi con la stessa polarità, sia la polarità dei bit di suddetta sequenza NV, la quale deve essere opposta a quella del bit bt_{j-6}, nel caso in cui il frame MF debba essere corrotto.

Come detto l'altra operazione fondamentale eseguita dal dispositivo di protezione 26 è l'oscuramento F2 al nodo CAN malevolo che trasmette il messaggio CAN non lecito intercettato dal dispositivo di protezione 26 della corruzione di tale messaggio CAN non lecito da lui stesso trasmesso, e quindi del suo conseguente blocco da parte dei controlli d'integrità nei controllori CAN degli altri nodi CAN.

Nel caso in cui il dispositivo di protezione 26 corrompa un frame non lecito MF, se il dispositivo di protezione 26 non nascondesse la corruzione, (ovvero la sequenza NV inserita in un punto di inserzione bt_{j-5} del campo CRC S5 del frame non lecito MF e la quale determina la condizione di Stuff error SPE al punto bt_j), il nodo CAN

mittente del frame malevolo MF rivelerebbe tale condizione di Stuff error SPE e, come conseguenza, procederebbe alla interruzione della trasmissione del frame malevolo MF, alla trasmissione di un frame di tipo Errore EM (disallineato rispetto a tutti gli altri frame di tipo Errore inviati da tutti gli altri nodi riceventi) e successivamente tenterebbe di ritrasmettere il medesimo frame malevolo.

L'operazione di oscuramento F2 del processo di corruzione del messaggio in transito è gestita come illustrato in Figura 7, dove gli elementi "CAN Controller" 13 e "CAN Transceiver" 12 evidenziati sono quelli ad esempio appartenenti al nodo CAN protetto 11_1 su cui è installato il dispositivo di protezione 26 e tale nodo CAN protetto trasmette un messaggio malevolo MF (caso in cui lo host del nodo CAN su cui è installato il dispositivo di protezione 26 è stato violato). In particolare, poiché ogni bit del messaggio CAN MF trasmesso sulla linea di trasmissione CT viene anche riletto sulla linea di ricezione CR, il dispositivo di protezione 26 opera come segue, eseguendo l'operazione di corruzione, dopo che, come rappresentato in figura 7A, è stato individuato il frame malevolo MF in arrivo al dispositivo 26 sulla linea di trasmissione CT, del frame malevolo, in due fasi:

in una prima fase, rappresentata in figura 7B, dal lato host, ossia verso il nodo malevolo, (linee di trasmissione CT e di ricezione filtrata DR), il messaggio CAN non lecito MF è replicato senza alcuna alterazione del bitstream sulla linea di ricezione filtrata DR, mentre dal lato CAN bus a valle del ricetrasmettitore 12, ossia verso nodi riceventi non malevoli, ossia sulla linea di trasmissione filtrata DT e sulla linea di ricezione non filtrata CR, il messaggio non lecito MF viene corrotto in

maniera opportuna modificandone il bitstream, come messaggio corrotto MF';

in una seconda fase, rappresentata in figura 7C, dal lato host, ossia verso il nodo malevolo, il dispositivo di protezione 26 emula il bus CAN segnalando la corretta ricezione del messaggio da parte degli altri nodi $11_2 \ldots 11_n$ della rete 20, tramite un messaggio di corretta ricezione OR sulla linea di DR (figura 7C), in particolare tramite l'invio del bit dominante durante il bit time ACK Slot; contemporaneamente, dal lato CAN bus, il dispositivo di protezione 26 blocca la segnalazione di errore, tramite Error Frame EM previsto dal protocollo CAN, sulla linea CR ad opera degli altri nodi 11 della rete che hanno ricevuto il messaggio corrotto MF'.

L'operazione di oscuramento F2 del processo di corruzione del messaggio in transito si applica anche al caso di messaggio non lecito in ricezione, ovvero trasmesso da un nodo CAN 11_1, diverso dal nodo CAN protetto 11_1 su cui è installato il dispositivo di protezione 26, in maniera analoga a quanto sopra espresso e da quanto riportato dalle figure 7A, 7B e 7C, in conformità alle caratteristiche del protocollo CAN in caso di ricezione di messaggio. In particolare, il messaggio MF da replicare verso il nodo malevolo, che dovrebbe essere per dualità trasmesso su DT in questo caso non è necessario, ossia non si adotta nessuna azione di replica, ma è sufficiente un messaggio di corretta ricezione OR a testimonianza di corretta ricezione del messaggio malevolo (che questa volta è sul CAN bus 10).

Dunque, il procedimento di protezione da attacchi informatici in una rete di comunicazione CAN (Controller Area Network) 20 di un veicolo comprendente un bus CAN 10 e

una pluralità di nodi 11 associati a detto bus CAN 10 in rapporto di scambio di segnale e associati almeno in parte a unità di controllo di funzioni del veicolo, comprendente le operazioni di analizzare il contenuto di messaggi CAN M in transito fra nodi di detta pluralità di nodi 11 per identificare messaggi CAN non leciti MF, e bloccare tramite le modalità B1, B2 detti messaggi non leciti MF, dove tale operazione di bloccare tramite le modalità B1, B2 comprende di rendere non validi i messaggi non leciti MF, ossia corrompere F1, rispetto a una verifica di integrità eseguita da un controllore CAN 13, di detti nodi 11, inserendo F1 una sequenza di bit NV di corruzione riconosciuta come un errore da detto controllore CAN 13, ottenendo un messaggio corrotto MF', prevede specificamente di inserire F1 detta sequenza di bit NV di corruzione in un campo di controllo integrità S5, in particolare un campo CRC, del messaggio CAN non lecito MF a un tempo di bit bt_{j-5} il cui valore è tale da allineare temporalmente un campo separatore, ossia ITM, del messaggio non lecito con un corrispondente campo separatore di un messaggio d'errore EM generato da un nodo della rete 20 che riceve detto messaggio non lecito MF comprendente detta sequenza di corruzione NV. Si noti che tale operazione di inserire è effettuata sostituendo parte della sequenza originale di bit, in particolare del campo di controllo integrità S5, con una di corruzione, la sequenza di bit NV, in particolare tale sequenza di bit NV avendo polarità opposta alla polarità del bit al tempo bt_{j-6} precedente il bit al punto di inserzione bt_{j-5}, ottenendo un messaggio corrotto o non lecito MF.

Il procedimento descritto comprende poi di

estrarre un contenuto informativo del messaggio M in transito durante la trasmissione;

- operare l'analisi di detto contenuto informativo detto contenuto informativo in base a un insieme di regole di firewall (R),

- rendere non valido F1 il messaggio M qualora detta analisi del contenuto informativo identifichi il messaggio (M) analizzato come messaggio non lecito MF ottenendo un messaggio corrotto MF'.

Il procedimento descritto comprende poi di selezionare se applicare l'operazione di rendere non valido F1 il messaggio non lecito MF almeno secondo una modalità di blocco selettiva B1 a tutti e soli i messaggi CAN MF non leciti o secondo una modalità di blocco totale B2 a tutti i messaggi CAN, leciti M e non leciti MF.

Il procedimento descritto comprende poi che detta operazione di rendere non valido il messaggio non lecito MF comprenda un'operazione di oscurare F2 al nodo CAN o rete CAN che trasmette il messaggio CAN MF non lecito detta operazione di inserzione di bit NV di corruzione, tramite i passi di

replicare detto messaggio CAN non lecito MF senza alcuna alterazione, in particolare senza sequenza NV, verso il nodo CAN 11 che trasmette detto messaggio non lecito MF, oppure non adottare nessuna azione di replica verso la rete CAN 10 che trasmette detto messaggio non lecito MF,

emulare il bus CAN 10 oppure il nodo CAN 11 per il caso di trasmissione del messaggio non lecito da parte di CAN 11 o bus CAN 10, rispettivamente segnalando la corretta ricezione del messaggio non lecito MF da parte di un nodo ricevente o nodi riceventi e contemporaneamente bloccare messaggi di errore EM associati a detto messaggio non

lecito MF a detto nodo CAN o rete CAN che trasmette detto messaggio non lecito.

Tali operazioni sono implementate dal dispositivo di protezione 26, in particolare dal suo modulo di firewall 261 in base alle regole R memorizzate nel modulo di memorizzazione 262.

Il dispositivo di protezione 26 a questo scopo può essere in forme varianti è disposto fra un controllore CAN 13 e un ricetrasmettitore CAN 12 di un nodo CAN, che è così un nodo protetto, anche dovesse essere il medesimo nodo malizioso.

Il dispositivo di protezione 26 può essere in ulteriori forme varianti disposto interposto fra due reti CAN 20A, 20B in associazione a un gateway 18.

Il dispositivo di protezione 26 dispone come detto di una interfaccia di configurazione, l'interfaccia 264 che consente la definizione delle regole R di firewall tramite le seguenti liste e parametri:

- "white-list", ossia lista di elementi abilitati o ammessi, per i messaggi ammessi (per ciascuna direzione) da applicare in determinate condizioni veicolo. Ogni voce di questa lista comprende i seguenti campi:
  a) identificativo;
  b) lunghezza;
  c) parametri di trasmissione e di soglia di violazione;
  d) Tipo di messaggio (diagnostico/non-diagnostico)
- "white-list dei servizi diagnostici" ammessi (applicabile solo ai messaggi di tipo diagnostico);
- "black-list, ossia lista di elementi non abilitati o non ammessi, dei servizi diagnostici" non ammessi

(applicabile solo ai messaggi di tipo diagnostico) da applicare in determinate condizioni veicolo;

- "soglie di violazioni delle white/black list" per attivare la modalità di blocco totale;
- "soglie di occupazione del bus" per attivare la modalità di blocco totale;

"informazioni di rilevamento condizione veicolo" per determinare quale sia lo stato (ad es. velocità attuale maggiore di 5km/h) da usare congiuntamente alla "black-list dei servizi diagnostici" e alla "white list" dei messaggi ammessi.

Le regole di firewall R impostate mediante i parametri e le liste sopra riportate sono immagazzinate nelle tabelle del modulo di memorizzazione 262 e possono essere aggiornate aggiungendo nuove regole di firewall R oppure sovrascrivendo e/o eliminando le esistenti regole di firewall R. Il dispositivo di protezione 26 nel modulo di memorizzazione 263 memorizza tutte le informazioni B statistiche relative all'attività del firewall (quantità di frame non leciti corrotti sulla linea DT, quantità di frame non leciti corrotti sulla linea DR, etc …) e che possono essere consultate mediante l'interfaccia di configurazione 264 che può accedere al modulo 263 come indicato in figura 5.

L'applicazione delle regole di firewall R definite e contenute nel modulo di memorizzazione 262 è attuata per ogni messaggio CAN M di tipo Data frame o Remote frame. Una rappresentazione schematica del processo di filtraggio è rappresentata in Figura 8.

In accordo con il diagramma di flusso di figura 8, è descritta una forma realizzativa d'esempio di procedura di protezione 100 eseguita dal dispositivo di protezione 26.

Dopo un avvio 105 della procedura, in un passo 110 dal campo Arbitration S2 del messaggio CAN in transito M il firewall 261 estrae un identificativo messaggio (ID 11 / 29 bit), che viene confrontato con il relativo campo della "white-list" per la condizione del veicolo impostata. Se tale identificativo messaggio è presente si procede con il passo successivo 120, altrimenti il messaggio M viene considerato non lecito MF e si procede con il passo 180.

Al passo 120 dal campo Control S3 del messaggio CAN in transito M il firewall 261 estrae una lunghezza messaggio (DLC 4 bit), che viene confrontata con il relativo campo della "white-list". Se la lunghezza è corretta si procede con il passo successivo 130, altrimenti il messaggio CAN M viene considerato messaggio non lecito MF e si procede con il passo 180.

Al passo 130 viene misurato il tempo intercorso dall'ultima ricezione dello stesso messaggio, in base all'identificativo, e viene confrontato con delle soglie di temporizzazione configurate (ad esempio un intervallo di tempo definito fra un tempo massimo Tmax e uno minimo Tmin, o tramite un periodo etc, anche in relazione alla cronologia delle violazioni delle regole di temporizzazione. Se il tempo intercorso dall'ultima ricezione dello stesso messaggio risulta ricadere in un intervallo ammesso oppure non è nell''intervallo ammesso, ma il numero di violazioni rilevate è inferiore a un valore di soglia definita (parametri tutti estratti dalla "white list", come quelli di intervallo di tempo) si procede con il passo successivo 135 altrimenti il messaggio CAN M viene considerato messaggio non lecito MF e si procede con il passo 180.

In tale passo 135 viene verificato se il messaggio M è

di tipo diagnostico. In caso negativo si passa a un passo 160 di aggiornamento dello stato del veicolo. In caso affermativo, dal campo *Data* in un passo 140 viene estratto il valore del servizio diagnostico e controllato che sia presente nella "white-list dei servizi diagnostici" memorizzata nel modulo 262. Se presente si procede con il passo successivo 150 altrimenti il messaggio CAN M viene considerato messaggio non lecito MF e si procede con il passo 180.

Successivamente, nel passo 150 dal campo Data S4 viene estratto il valore del servizio diagnostico e controllato che non sia presente nella "black-list dei servizi diagnostici" per la condizione del veicolo impostata (si veda passo 160). Se presente il messaggio M viene considerato messaggio non lecito MF passando al passo 180, altrimenti lecito e si passa al passo 160 di aggiornamento dello stato del veicolo.

In tale passo 160, impiegando "informazioni di rilevamento condizione veicolo" congiuntamente ai campi di *Arbitration* e *Data del messaggio M* viene aggiornata l'informazione interna che rappresenta la condizione del veicolo. Specificamente, il passo 160 verifica se è necessario effettuare l'aggiornamento dello stato del veicolo. Il fattore discriminante per valutare se deve essere aggiornato lo stato del veicolo è contenuta nell'insieme delle regole R. La verifica si basa sui campi Arbitration e Data del frame in transito.

Quindi, in un passo 170, dalla lunghezza totale del messaggio viene aggiornato il valore dell'occupazione del bus e confrontato con le "soglie di occupazione del bus". Se il messaggio non rispetta tali soglie il messaggio CAN M viene considerato messaggio non lecito MF e si procede con

il passo 180. Viceversa la procedura 100 in un passo 195 ha termine.

Dunque, in generale, le operazioni del firewall 261 di estrarre il contenuto informativo di un messaggio CAN M transitante sulle linee di trasmissione CT o ricezione CR e operare l'analisi di tale contenuto informativo, comprendono una o più delle operazioni 110, 120, 130, 135, 140, 150, 170.

Nel passo 180, poiché il messaggio CAN M è considerato messaggio non lecito MF, viene determinato, combinando il tipo di violazione rilevata con le "soglie di violazioni delle white/black list" viene determinato se attivare la modalità di blocco B1 o B2.

Nel passo 190, le informazioni di validità del messaggio e della modalità di blocco B1 o B2 da attuare vengono trasmesse al blocco 261 di firewall che provvede a eseguire le operazioni richieste dalla modalità di blocco, ossia blocco totale (B1) oppure operazione di blocco tramite corruzione F1 e di oscuramento F2 (B2).

Il dispositivo di protezione 26 prevede di operare sia con messaggi diagnostici single-frame sia con messaggi multi-frame. Nel caso di messaggi diagnostici multi-frame, se viene riconosciuto come malevolo il primo frame della catena di messaggi, il dispositivo di protezione 26 è in grado di bloccare tale messaggio e tutti i messaggi successivi che compongono il messaggio multi-frame, attraverso il passo 135. Di conseguenza, sono presenti all'interno del dispositivo di protezione 26 contatori per tenere traccia di quanti CAN frame sono transitati sul CAN bus, e determinare quando terminare il processo di corruzione per uno specifico servizio diagnostico.

Dunque, da quanto descritto sopra, sono chiari i vantaggi della soluzione proposta.

Il dispositivo e procedimento descritti permettono di evitare il disallineamento temporale tra il messaggio corrotto (inviato sul bus) ed il messaggio "Error-Frame" generato dal nodo CAN che riceve il messaggio corrotto.

Il dispositivo e il procedimento descritti permettono inoltre, mediante un opportuno processo di offuscamento, di mascherare l'operazione di corruzione al nodo CAN che ha inviato il frame non lecito. In questo modo si evita la ritrasmissione automatica, con conseguente occupazione del CAN bus, da parte del nodo CAN malevolo.

Il dispositivo e procedimento descritti permettono di non introdurre alcun ritardo di propagazione dei messaggi CAN garantendone l'utilizzo in modo trasparente da parte dei nodi CAN coinvolti.

Il dispositivo e il procedimento descritti permettono di operare anche con i messaggi CAN di tipo diagnostico. Grazie ad una logica di controllo dedicata si è in grado di riconoscere una sequenza di messaggi diagnostici di tipo multi-frame ed invalidare, se il servizio diagnostico è identificato come malevolo, tutta la catena di messaggi.

RIVENDICAZIONI

1. Procedimento di protezione da attacchi informatici in una rete di comunicazione CAN (Controller Area Network) (20) di un veicolo comprendente un bus CAN (10) e una pluralità di nodi (11) associati a detto bus CAN (10) in rapporto di scambio di segnale e associati almeno in parte a unità di controllo di funzioni del veicolo,

comprendente le operazioni di

analizzare il contenuto di messaggi CAN (M) in transito fra nodi di detta pluralità di nodi (11) per identificare messaggi CAN non leciti (MF),

bloccare (B1, B2) detti messaggi non leciti (MF),

detta operazione di bloccare (B1, B2) comprendendo di rendere non validi (F1, F2) detti messaggi non leciti (MF) rispetto a una verifica di integrità eseguita da un controllore CAN (13) di detti nodi (11), inserendo (F1) una sequenza di bit (NV) di corruzione riconosciuta come un errore da detto controllore CAN (13), ottenendo un messaggio corrotto (MF'),

caratterizzato dal fatto di

inserire (F1) detta sequenza di bit (NV) di corruzione in un campo di controllo integrità (S5), in particolare un campo CRC, del messaggio CAN non lecito (MF) a un tempo di bit (bt_{j-5}) il cui valore è tale da allineare temporalmente un campo separatore (ITM) del messaggio non lecito con un corrispondente campo separatore di un messaggio d'errore (EM) generato da un nodo della rete (20) che riceve detto messaggio non lecito (MF) comprendente detta sequenza di corruzione (NV).

2. Procedimento secondo la rivendicazione 1, caratterizzato dal fatto che comprende di

estrarre un contenuto informativo del messaggio (M) in transito durante la trasmissione;

- operare l'analisi di detto contenuto informativo detto contenuto informativo in base a un insieme di regole di firewall (R),

- rendere non valido (F1, F2, 190) detto messaggio (M) qualora detta analisi del contenuto informativo identifichi il messaggio (M) analizzato come messaggio non lecito (MF) ottenendo un messaggio corrotto (MF').

3. Procedimento secondo la rivendicazione 1, caratterizzato dal fatto di selezionare (180) se applicare detto operazione di rendere non valido (F1, F2, 190) il messaggio non lecito (MF) almeno secondo una modalità di blocco selettiva (B1) a tutti e soli i messaggi CAN (MF) non leciti o secondo una modalità di blocco totale (B2) a tutti i messaggi CAN (M, MF).

4. Procedimento secondo una delle rivendicazioni da 1 a 3, caratterizzato dal fatto che detta operazione di rendere non valido (F1, F2, 190) detto messaggio (MF) non lecito comprende un'operazione di oscurare (F2) al nodo CAN (11) o rete CAN (10) che trasmette il messaggio CAN (MF) non lecito detta operazione di inserzione di una sequenza di bit (NV) di corruzione, tramite i passi di

replicare detto messaggio CAN non lecito (MF) senza alcuna alterazione verso il nodo CAN (11) che trasmette detto messaggio non lecito (MF) oppure non adottare nessuna azione di replica verso la rete CAN (10) che trasmette detto messaggio non lecito (MF),

emulare il bus CAN (10) oppure il nodo CAN (11) per il caso di trasmissione del messaggio non lecito da parte di CAN (11) o rete CAN (10), rispettivamente segnalando la corretta ricezione del messaggio non lecito (MF) da parte

di un nodo ricevente o nodi riceventi e contemporaneamente bloccare messaggi di errore (EM) associati a detto messaggio non lecito (MF) a detto nodo CAN (11) o rete CAN (10) che trasmette detto messaggio non lecito (MF).

5. Procedimento secondo una delle rivendicazioni da 2 a 4, caratterizzato dal fatto che detto insieme di regole (R) di firewall comprende uno o più dei seguenti liste e parametri:

- white-list per i messaggi ammessi da applicare in determinate condizioni veicolo;
- white-list dei servizi diagnostici ammessi;
- black-list dei servizi diagnostici non ammessi da applicare in determinate condizioni veicolo;
- soglie di violazioni delle white list e black list per attivare la modalità di blocco totale (B2);
- soglie di occupazione del CAN bus (10) per attivare la modalità di blocco totale (B2);
- informazioni di rilevamento condizione veicolo indicative delle condizioni veicolo da impiegare per valutare detta black-list dei servizi diagnostici e detta "white list" dei messaggi ammessi.

6. Procedimento di protezione secondo la rivendicazione 5, caratterizzato dal fatto che comprende una o più delle seguenti operazioni di analisi del contenuto informativo del messaggio CAN (M)

- estrarre (110) un identificativo messaggio e confrontare con un campo corrispondente di una white-list per una data condizione del veicolo;

- estrarre (120) una lunghezza messaggio che viene confrontata con un campo corrispondente di un white list, con il relativo campo della white-list

- misurato (130) di un tempo intercorso dall'ultima

ricezione dello stesso messaggio e confronto con soglie di temporizzazione

a) verifica, se il messaggio è di tipo diagnostico, della presenza in una white-list dei servizi diagnostici
b) estrazione, se il messaggio è di tipo diagnostico, del valore del servizio diagnostico e verifica della presenza in una "black-list dei servizi diagnostici" per una data condizione del veicolo.

- verifica di un valore dell'occupazione del bus e confronto con delle soglie di occupazione del bus.

7. Procedimento di protezione secondo una delle rivendicazioni precedenti, caratterizzato dal fatto che l'ultimo bit (bt_{j-6}) immediatamente precedente al primo bit (bt_{j-5}) della sequenza di corruzione (NV) ha polarità opposta rispetto a detto primo bit (bt_{j-5}) della sequenza di corruzione (NV).

8. Dispositivo di protezione da attacchi informatici in una rete di comunicazione CAN (Controller Area Network) (20) di un veicolo comprendente un bus CAN (10) e una pluralità di nodi (11) associati a detto bus CAN (10) in rapporto di scambio di segnale e associati almeno in parte a unità di controllo di funzioni del veicolo, caratterizzato dal fatto di essere configurato per operare secondo il procedimento secondo una o più delle rivendicazioni da 1 a 7.

9. Dispositivo di protezione secondo la rivendicazione 8, caratterizzato dal fatto che comprende un modulo di firewall (261) configurato per eseguire almeno dette operazioni di

analizzare il contenuto di messaggi CAN (M) e rendere non validi (F1, F2) messaggi non leciti (MF) rispetto a una verifica di integrità eseguita da un controllore CAN (13) di detti nodi (11),

e un modulo di memorizzazione per memorizzare detto insieme di regole (R) del firewall.

10. Dispositivo di protezione secondo la rivendicazione 8 o 9, caratterizzato dal fatto che

detto dispositivo di protezione (26) è disposto fra un controllore CAN (13) e un ricetrasmettitore CAN (12) di un nodo CAN.

11. Dispositivo di protezione secondo la rivendicazione 8 o 9, caratterizzato dal fatto che

detto dispositivo di protezione (26) è disposto interposto fra due reti CAN (20A, 20B) in associazione a un gateway (18).

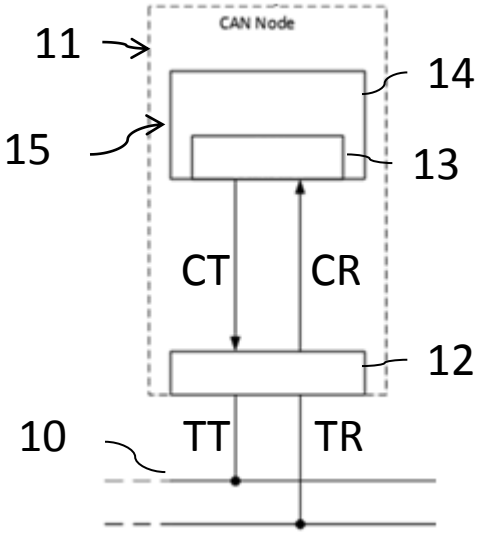
CAN Node
11
14
15
13
CT
CR
12
10
TT
TR

Fig. 1A

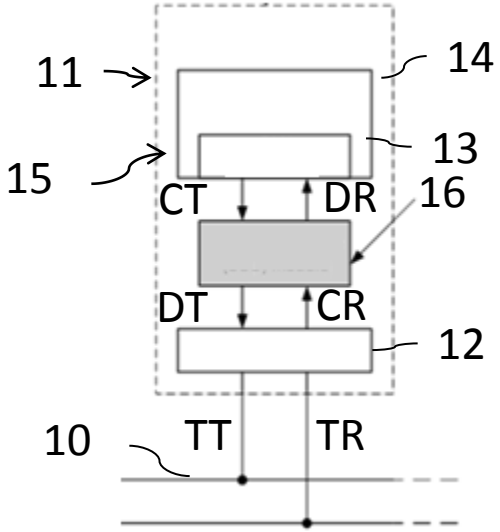
11
14
13
15
CT
DR
16
DT
CR
12
10
TT
TR

Fig. 1B

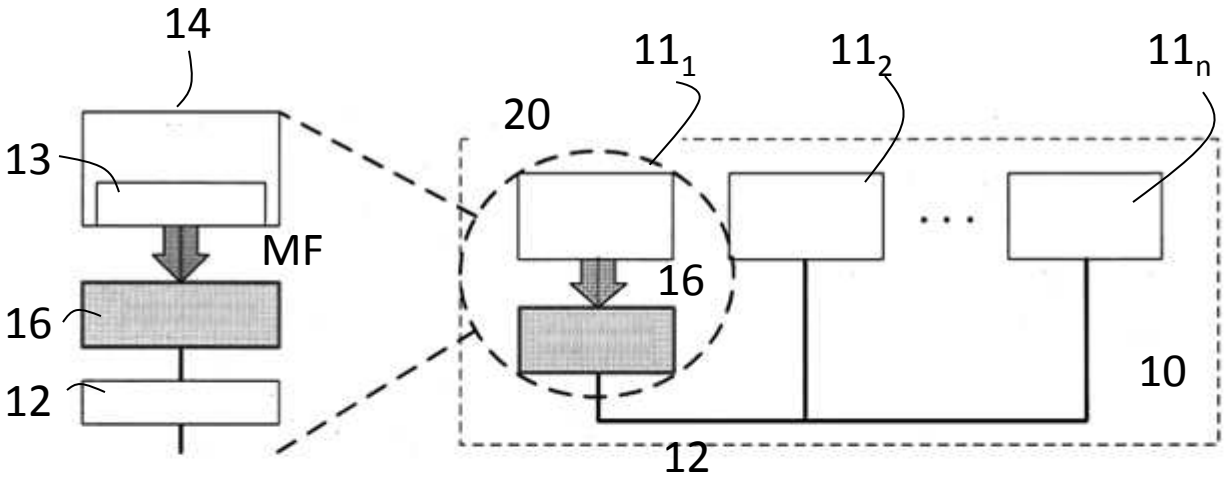
14
13
MF
16
12
20
11_1
11_2
11_n
16
10
12

Fig. 2

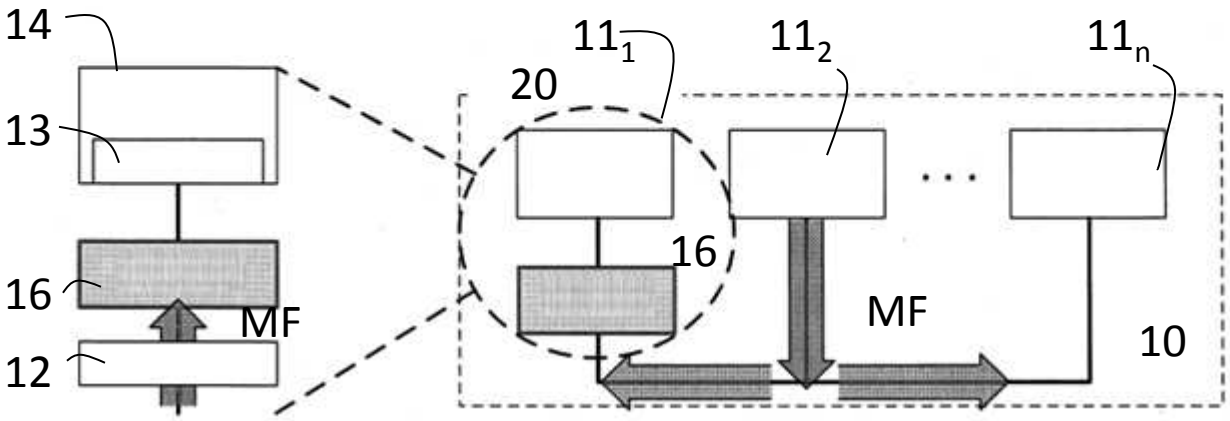
14
13
16
MF
12
20
11_1
11_2
11_n
16
MF
10

Fig. 3

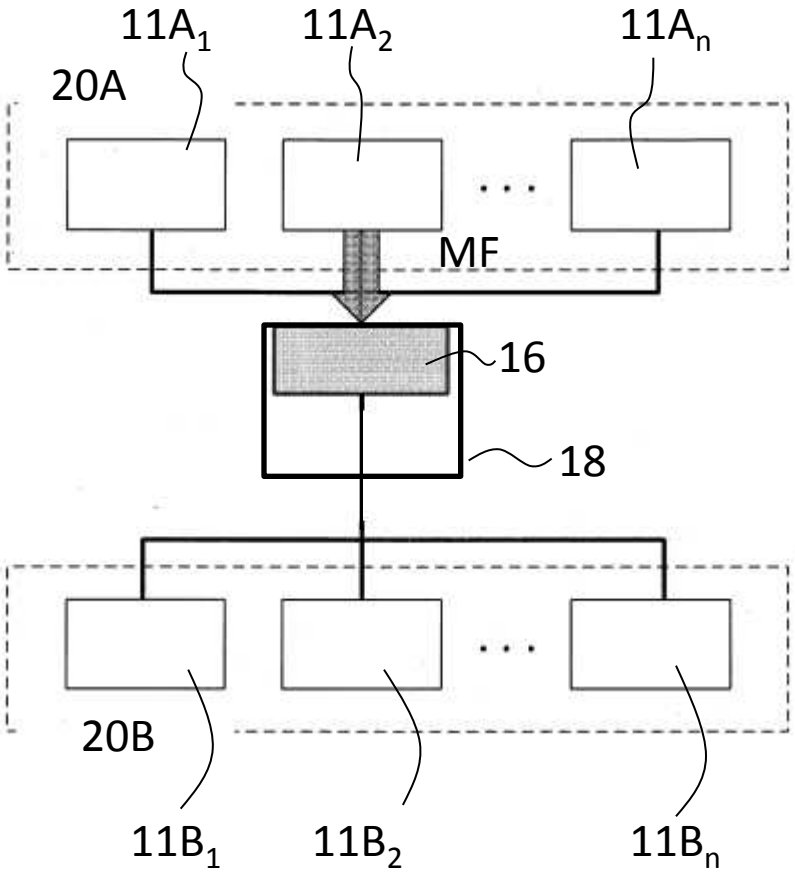

Fig. 4

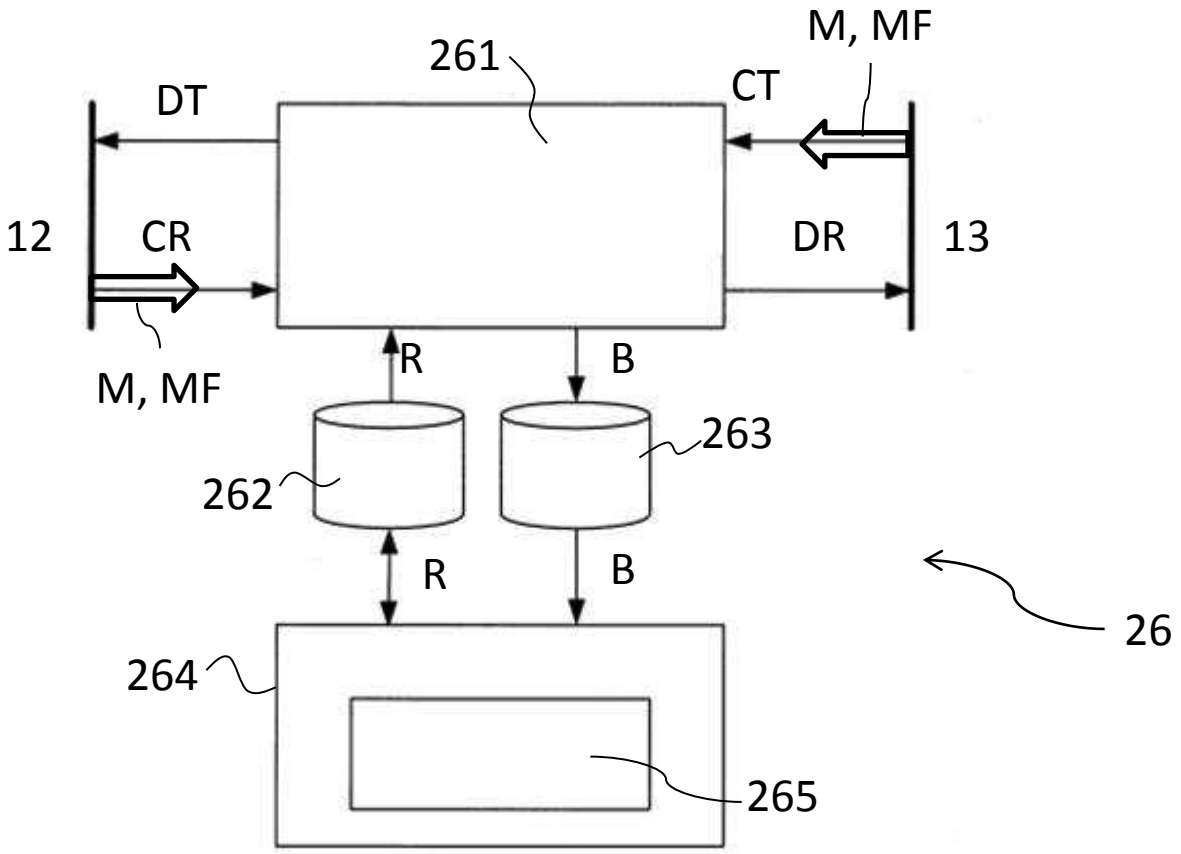

Fig. 5

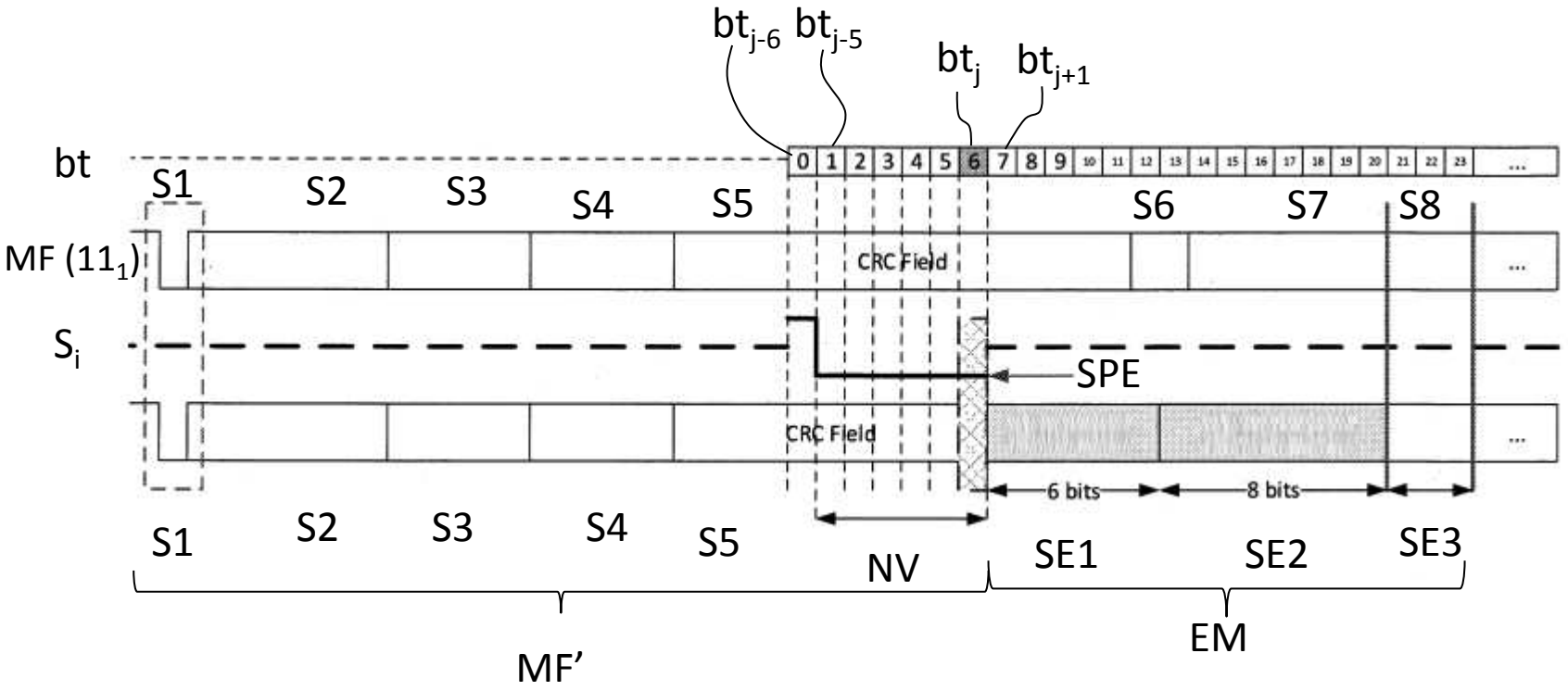
bt
MF (11₁)
Sᵢ
btj-6
btj-5
btj
btj+1
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 ...
S1
S2
S3
S4
S5
S6
S7
S8
CRC Field
SPE
6 bits
8 bits
NV
SE1
SE2
SE3
MF'
EM

Fig. 6

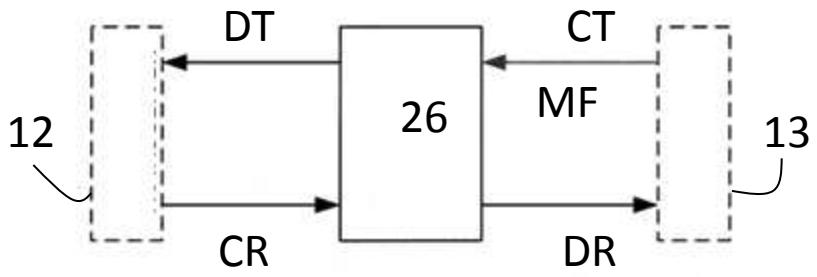

Fig. 7A

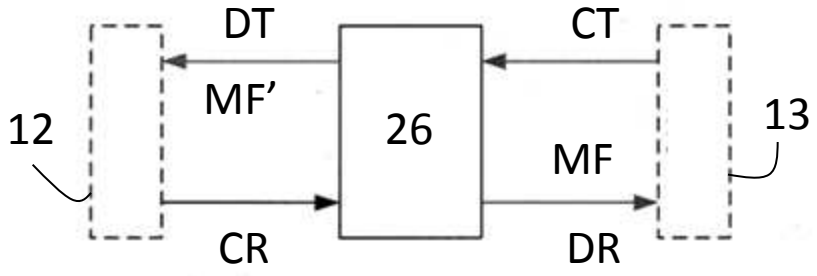

Fig. 7B

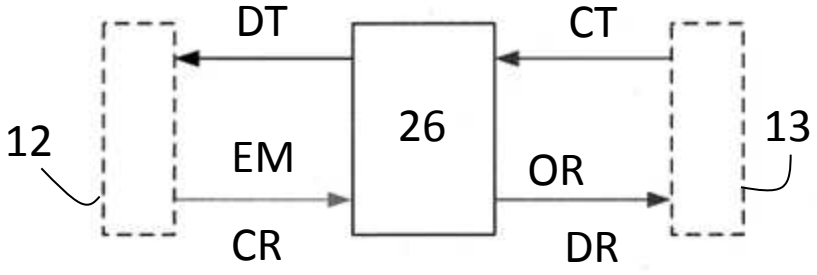

Fig. 7C

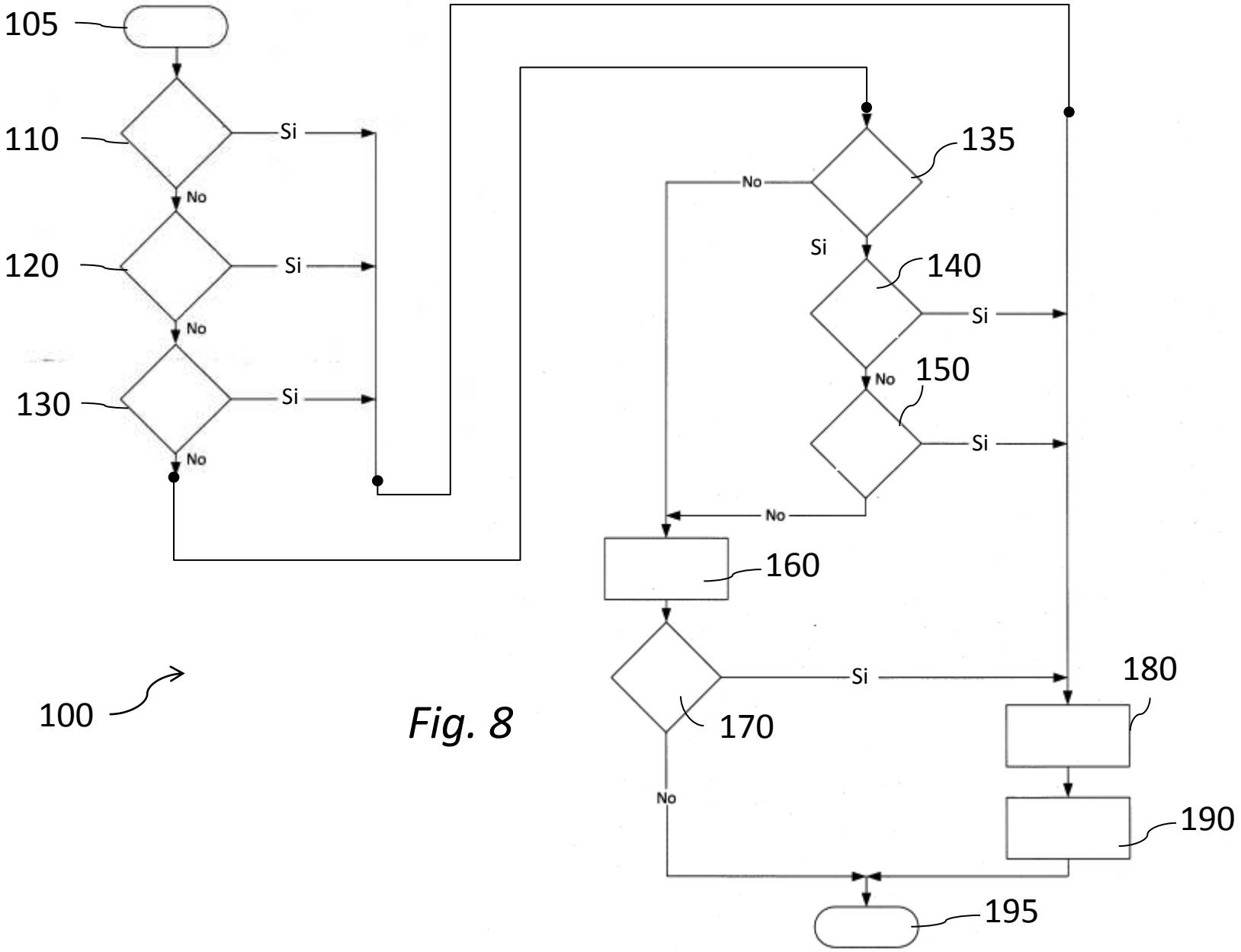
105
110
Si
No
120
Si
No
130
Si
No
135
No
Si
140
Si
No
150
Si
No
160
Si
170
No
180
190
195
100

Fig. 8

Ministero dello Sviluppo Economico
DIREZIONE GENERALE SVILUPPO PRODUTTIVO E COMPETITIVITA'-
UFFICIO ITALIANO BREVETTI E MARCHI

RAPPORTO DI RICERCA

Numero della domanda
IO 88140
IT 201800021550

DOCUMENTI CONSIDERATI DI RILIEVO

Categoria	Citazione del documento con indicazione, se appropriata, delle parti rilevanti	Rivendicazioni rilevanti	CLASSIFICAZIONE DELLA DOMANDA (IPC)
X,D	US 2015/191136 A1 (BEN NOON OFER [IL] ET AL) 9 July 2015 (2015-07-09) * abstract * * paragraph [0051] - paragraph [0108] * * figures 1A, 2A, 2B, 2C * * paragraph [0027] - paragraph [0036] * -----	1-11	INV. H04L1/00 G06F21/55 G06F21/60
A	US 8 788 731 B2 (PEIRCE KENNETH L [US]; FOREST THOMAS M [US] ET AL.) 22 July 2014 (2014-07-22) * abstract * * column 7, line 37 - column 10, line 3 * -----	1-11	
A	KWON HYEOKCHAN ET AL: "Mitigation mechanism against in-vehicle network intrusion by reconfiguring ECU and disabling attack packet", 2018 INTERNATIONAL CONFERENCE ON INFORMATION TECHNOLOGY (INCIT), MAHASARAKHAM UNIVERSITY, FACULTY OF INFORMATICS, 24 October 2018 (2018-10-24), pages 1-5, XP033483124, DOI: 10.23919/INCIT.2018.8584882 [retrieved on 2018-12-20] * abstract * -----	1-11	

CAMPI TECNICI RICERCATI (IPC)
H04L
G06F

Questo rapporto di ricerca è stato redatto sulla base di tutte le rivendicazioni

Munich	Data di completamento della ricerca 13 September 2019	Esaminatore Garrammone, Giuliano

CATEGORIA DEI DOCUMENTI CITATI

X : di particolare rilevanza se considerato singolarmente
Y : di particolare rilevanza se combinato con un altro documento della stessa categoria
A : informazione generica
O : divulgazione orale
P : documento intermedio

T : teoria o principio alla base dell'invenzione
E : documento brevettuale antecedente, ma pubblicato dopo o alla data di deposito
D : documento citato nella domanda
L : documento citato per altre ragioni
.....
& : membro della stessa famiglia di brevetti, documento corrispondente

EPO FORM 1503 07.08 (P04C74)

ALLEGATO AL RAPPORTO DI RICERCA SULLA DOMANDA DI BREVETTO ITALIANO N.

IO 88140
IT 201800021550

Questo allegato enumera i membri della famiglia di brevetti relativi a documenti brevettuali citati nel summenzionato rapporto di ricerca.
I membri sono indicati come da database dell'Ufficio Europeo dei Brevetti al 13-09-2019
L'Ufficio Europeo dei Brevetti non si assume alcuna responsabilità per queste indicazioni, che vengono fornite a solo scopo informativo.

Documenti brevettuali citati nel rapporto di ricerca	Data di pubblicazione	Membri della famiglia di brevetti	Data di pubblicazione
US 2015191136 A1	09-07-2015	EP 2892199 A1	08-07-2015
		EP 2892200 A1	08-07-2015
		EP 2892201 A1	08-07-2015
		EP 2892202 A1	08-07-2015
		EP 3358800 A1	08-08-2018
		JP 6382724 B2	29-08-2018
		JP 6502561 B2	17-04-2019
		JP 2015136107 A	27-07-2015
		JP 2019013007 A	24-01-2019
		JP 2019115067 A	11-07-2019
		US 2015191135 A1	09-07-2015
		US 2015191136 A1	09-07-2015
		US 2015191151 A1	09-07-2015
		US 2015195297 A1	09-07-2015
		US 2017259761 A1	14-09-2017
		US 2017341604 A1	30-11-2017
		US 2017341605 A1	30-11-2017
		US 2017355326 A1	14-12-2017
		US 2018015888 A1	18-01-2018
		US 2018029539 A1	01-02-2018
		US 2018029540 A1	01-02-2018
		US 2019111863 A1	18-04-2019
US 8788731 B2	22-07-2014	NONE	

Ministero dello Sviluppo Economico

DIREZIONE GENERALE SVILUPPO PRODUTTIVO E COMPETITIVITA' -
UFFICIO ITALIANO BREVETTI E MARCHI

OPINIONE SCRITTA

N. dossier	Data di deposito *(gg/mm/aa)*	Data di priorità *(gg/mm/aa)*	N. domanda
IO88140	31.12.2018		IT201800021550

Classificazione Internazionale dei Brevetti (IPC)
INV. H04L1/00 G06F21/55 G06F21/60

Richiedente
MAGNETI MARELLI S.P.A., et al

Questa opinione fornisce indicazioni riguardanti i seguenti elementi:

- ☒ Riquadro N. I — Base dell'opinione
- ☐ Riquadro N. II — Priorità
- ☐ Riquadro N. III — Non-redazione di un'opinione a riguardo di novità, attività inventiva e applicazione industriale
- ☐ Riquadro N. IV — Violazione del requisito d'unità dell'invenzione
- ☒ Riquadro N. V — Dichiarazione motivata a riguardo di novità, attività inventiva o applicazione industriale; citazioni e spiegazioni giustificative della dichiarazione
- ☐ Riquadro N. VI — Particolari documenti citati
- ☒ Riquadro N. VII — Difetti particolari nella domanda
- ☒ Riquadro N. VIII — Osservazioni particolari a riguardo della domanda

	Esaminatore
	Garrammone, Giuliano

N. domanda

OPINIONE SCRITTA

IT201800021550

Riquadro N. I Base dell'opinione

1. Questa opinione è stata redatta sulla base delle ultime rivendicazioni depositate prima dell'inizio della ricerca nella tecnica anteriore.

2. Per quanto concerne eventuali sequenze di nucleotidi e/o amminoacidi descritte nella domanda e necessarie per l'invenzione di cui oggetto nelle rivendicazioni, questa opinione è stata redatta sulla base di:

   a. tipo di materiale:

   ☐ una sequenza di DNA

   ☐ una o più tabelle relative alla sequenza di DNA

   b. formato del materiale:

   ☐ cartaceo

   ☐ elettronico

   c. momento di deposito o presentazione:

   ☐ depositato insieme alla domanda al momento del deposito della medesima

   ☐ depositato insieme alla domanda in formato elettronico

   ☐ presentato successivamente al fine della ricerca d'anteriorità

3. ☐ Inoltre, ove sia stata depositata o presentata più di una versione o copia di una sequenza di DNA e/o tabella ad essa relativa, è stata presentata anche la dichiarazione obbligatoria che le informazioni contenute nelle copie successive o addizionali sono identiche a quelle nella domanda come depositata o che, in ogni caso, non vanno oltre il contenuto della domanda depositata originariamente.

4. Note aggiuntive:

N. domanda

OPINIONE SCRITTA

IT201800021550

Riquadro N. VDichiarazione motivata a riguardo di novità, attività inventiva o applicazione industriale; citazioni e spiegazioni giustificative della dichiarazione

1. 1. Dichiarazione

Novità (N)	Sì:	Rivendicazioni	3, 4, 6, 7
	No:	Rivendicazioni	1, 2, 5, 8-11
Attività inventiva (IS)	Sì:	Rivendicazioni	
	No:	Rivendicazioni	1-11
Applicazione industriale (IA)	Sì:	Rivendicazioni	1-11
	No:	Rivendicazioni	

2. 2. Citazioni e spiegazioni

si veda l'allegato

Riquadro N. VII Difetti particolari nella domanda

si veda l'allegato

Riquadro N. VIII Osservazioni particolari a riguardo della domanda

si veda l'allegato

1 **Re Item V**

Reasoned statement with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

Reference is made to the following document:

D1 US 2015/191136 A1 (BEN NOON OFER [IL] ET AL) 9 July 2015 (2015-07-09)

1.1 Notwithstanding the clarity objections, the present application does not meet the criteria of patentability, because the subject-matter of claim 1 is not new.

1.1.1 D1 discloses (references to D1 in parentheses): Method for protection from cyber attacks in a CAN communications network (20) of a vehicle comprising a CAN bus (10) and a plurality of nodes (11) associated to said CAN bus (10) in a signal exchange relationship and associated at least in part with vehicle functions control units (abstract; paragraph [0051] - paragraph [0108]; paragraph [0027] - paragraph [0036]; figures 1A, 2A, 2B, 2C; the method is performed in the Watchman device), comprising the operations of analyzing the content of CAN messages (M) in transit between nodes of said plurality of nodes (11) to identify not allowed CAN messages (MF), blocking (B1, B2) said not allowed CAN messages (MF), said blocking operation (B1, B2) comprising to make such not allowed CAN messages (MF) non valid (F1, F2) with respect to an integrity check performed by a CAN controller (13) of said nodes (11), introducing (F1) a corruption bit sequence (NV) recognized as error by said CAN controller (13), obtaining a corrupted messages (idem passage; with reference to figure 2C, not allowable messages are identified at e.g., block 154), characterized by introducing (F1) said corruption bit sequence (NV) in an integrity check field, in particular a CRC field (idem passage; in particular, figure 2C, paragraph [71]; see also clarity objection at item 3.1), of the not allowed CAN message (MF) at a bit time (bt_{j-5}) which value is such to align in time a separating field (ITM) of the not allowed CAN messages with a corresponding separating field of an error message (EM) generated by a node of the

network (20) which receives said not allowed CAN message (MF) comprising said corruption sequence (idem passage; see also clarity objection at items 3.2, 3.3).

1.1.2 Therefore, the subject-matter of independent method claim 1 is known from document D1. The corresponding independent apparatus claim 8 related to the implementation of the method in terms of corresponding apparatus features is considered as implicitly disclosed by document D1, *mutatis mutandis*.

1.2 Dependent claims 2-7, 9-11

1.2.1 Claims 2, 9: D1 discloses poisoning of a message if it does not meet specific rules, which are considered the firewall rules (e.g., figure 2C, items 154, 171).

1.2.2 Claims 3, 4, 6, 7 do not appear to contain any additional features which, in combination with the features of any claim to which they refer, meet the requirements of inventive step because are simple implementation details.

1.2.3 Claim 5: the use of white and black lists is disclosed by D1 (paragraphs [57], [73]).

1.2.4 Claim 10: D1 discloses integration of watchman between controller and transceiver (paragraph [27]).

1.2.5 Claim 11: D1 discloses watchman connected to CAN gateway (paragraph [52]).

2 **Re Item VII**

Certain defects in the application

2.1 The description should be in conformity with the claims.

2.2 Abbreviations between brackets are not considered to be reference signs. Such abbreviations should be put between commas.

3 **Re Item VIII**

Certain observations on the application

3.1 Independent claims 1, 8 lack clarity with respect to the features

"a bit time (bt_{j-5}) which value is such to align in time a separating field (ITM) of the not allowed CAN messages with a corresponding separating field of an error message (EM) generated by a node of the network which receives said not allowed CAN message (MF) comprising said corruption sequence (NV)"

because it is not clear which are the technical features defining said separating fields (see e.g. figure 6 of the description). Moreover, the reference sign "ITM" cannot be found in any drawing.

3.2 Independent claims 1, 8 lack clarity with respect to the term "in particular". Expressions of this kind have no limiting effect on the scope of a claim; that is to say, the feature following any such expression is to be regarded as entirely optional.

3.3 Given the above-mentioned clarity issues, the interpretation of the unclear claims has been done omitting the unclear terms.

Franco Buzzi
Giancarlo Notaro
Enrico Antonielli d'Oulx
Luciano Bosotti
Mauro Marchitelli
Livia Pasqualigo
Franco Gallarotti
Cristina Freyria Fava
Alessandra Romeo
Giorgio Crovini
Stefano Frontoni
Tassilo Meindl
Antonella Vitale
Davide Resmini
Paolo De Bonis
Roberta Cesa
Loredana Mansi
Gianluca Notaro
Nemio Giuliano
Filippo Buzzi
Ilaria Gallo
Alberto Ferrero
Giovanna Campogiani

Ministero dello Sviluppo Economico
DIPARTIMENTO PER L'IMPRESA E L'INTERNAZIONALIZZAZIONE
Direzione Generale per la lotta alla contraffazione - UIBM
Ufficio Italiano Brevetti e Marchi – Divisione XI

29 settembre 2020

Prot. N. mise.AOO_PIT.REGISTRO UFFICIALE.U.0275489.27-09-2019
Ns. Rif.: BIT21850-GC

OGGETTO: Domanda n. 102018000021550. Procedimento di esame.

La presente dà riscontro entro il termine prescritto di 18 più 3 mesi dalla data di priorità del 31 dicembre 2020.

* * *

1. Contenuto del rapporto di ricerca e dell'opinione sulla brevettabilità

Nel rapporto di ricerca inviato unitamente a tale comunicazione, nel Riquadro N. V era indicata, per le rivendicazioni da 3, 4, 6 e 7 la presenza del requisito di novità. Era invece indicata l'assenza del requisito di altezza inventiva per le rivendicazioni da 1 a 11. Le rivendicazioni, da 1 a 11 erano invece riconosciute suscettibili di applicazione industriale.

2. Riscontro dato al rapporto di ricerca e all'opinione sulla brevettabilità

Con la presente i sottoscritti mandatari provvedono:
- a depositare una stesura modificata delle rivendicazioni (pagine 29 - 33) con modifiche evidenziate unitamente a un testo delle rivendicazioni pulito,
- a produrre precisazioni sull'ammissibilità delle rivendicazioni emendate e sulla conformità delle stesse alle disposizioni dell'art. 76, comma 1, lettera c) del Codice della Proprietà Industriale, e
- a formulare considerazioni per cui i rilievi di carenze presenti nell'opinione di brevettabilità sulle rivendicazioni siano da ritenersi ingiustificati e, in ogni caso, superati con la stesura modificata come qui depositata.

3. Stesura modificata della descrizione e delle rivendicazioni ed ammissibilità delle modifiche

<u>Nelle rivendicazioni (pagine 29 -33):</u>
La rivendicazione 1 è stata modificata sulla base della descrizione, pagina 17, righe 27-31 e Tabella 1, per chiarire il significato di campo di separazione, come richiesto al punto 3.1. del parere allegato al rapporto di ricerca. Le espressioni

Buzzi, Notaro & Antonielli d'Oulx S.r.l. ▪ C.so Vittorio Emanuele II, 6 ▪ 10123 Torino, Italy ▪ Tel. + 39 011 8392911
Fax + 39 011 8392929 ▪ info@bnaturin.com ▪ Cap. Soc. € 100.000 ▪ C.F. / P.IVA (VAT IT) 06294960015
Uff. Reg. Imp. Trib. Torino 1830/92 ▪ REA C.C.I.A.A. Torino 776713 ▪ R.C. Italiana n. 6084941 - € 3.000.000

opzionali nel campo 'in particolare' sono state cancellate nelle rivendicazioni 1 e 8, come richiesto al punto 3.2 del parere allegato al rapporto di ricerca, così come è stata modificata l'esplicitazione degli acronimi (punto 2.2 del parere) nelle medesime rivendicazioni.

La stesura modificata non si estende quindi oltre il contenuto della domanda iniziale e risulta pertanto conforme all'art. 76, comma 1, lettera c) del Codice della Proprietà Industriale.

4. Osservazioni sulle carenze individuate nell'opinione sulla brevettabilità

L'opinione sulla brevettabilità indicava al paragrafo 1.1.2 come la rivendicazione 1 non sarebbe stata nuova a fronte del documento D1 (US 2015191136 A1). Altri due documenti erano citati puramente come sfondo tecnico dell'invenzione. Allo stesso al punto 3.1 l'Esaminatore europeo indicava di non avere chiara una caratteristica della parte caratterizzante. Si nota che infatti tale caratteristica in virtù di tale non comprensione non è indirizzata nell'analisi al punto 1.1.1 dell'opinione sulla brevettabilità (come affermato esplicitamente al punto 3.3) e si vogliono perciò qui sottomettere argomenti che indicano come la rivendicazione 1, in particolare come ora correntemente emendata, sia nuova e inventiva a fronte di tale documento e allo stato dell'arte citato.

4.1 Il documento D1 (US2015191136A1) si riferisce a una rete di comunicazione a bordo di un veicolo comprendente un bus e nodi collegati al bus. Il documento D1 descrive l'impiego di un dispositivo cosiddetto Watchman o guardiano, che monitora il traffico sulla rete del veicolo che può indicare disturbi o anomalie del funzionamento. Il documento D1 indica che per distruggere o bloccare un messaggio CN, il processore 41 può controllare il Watchman per trasmettere almeno un bit dominante che rimpiazza un bit del CRC del messaggio [D1, par. 0071].

Si deve qui specificare, con riferimento anche all'obiezione del punto 3.1, che l'Esaminatore, che indica come anticipatore il par. 0071, non ha tenuto in considerazione nella propria analisi (punto 1.1.1 del parere di brevettabilità) il fatto che l'inserimento dei bit nella domanda in oggetto, come rivendicato, avviene a un tempo di bit specifico, il cui valore permette di allineare un campo separatore. Anche se mi permetto di affermare che sia del tutto chiaro al tecnico del settore che '*campo separatore*' si riferisce in un bus come il CAN bus a un campo che separa un messaggio dall'altro, ora quest'aspetto è stato specificato per via di emendamento e risulta evidente che il documento D1, che non fa menzione di allineamento di campi di separazione, non indica di operare l'inseriremo di bit nel modo rivendicato, dunque il documento D1 non descrive "*inserire (F1) detta sequenza di bit (NV) di corruzione in un campo di controllo integrità (S5) del messaggio CAN non lecito (MF) a un tempo di bit (btj-5) il cui valore è tale da allineare temporalmente un campo separatore (ITM), comprendente una zona di bit recessivi che funge da separatore tra messaggi, del messaggio non lecito con un corrispondente campo separatore di un messaggio d'errore (EM) generato da un nodo della rete (20) che riceve detto messaggio non lecito (MF) comprendente detta sequenza di corruzione (NV)*".

Dunque la rivendicazione 1 è nuova rispetto al documento D1

Dunque la rivendicazione 1 è nuova rispetto allo stato dell'arte.

4.2 Venendo al livello inventivo, l'effetto delle differenze suindicate al punto 4.1 rispetto al documento D1, considerato come arte nota più vicina, è che l'inserimento

della sequenza di bit di corruzione come rivendicato permette di allineare tutti i nodi sul bus riguardo ai prossimi messaggi da inviare. Questa è una condizione necessaria per avere una corretta gestione del bus CAN. Non si può inviare un nuovo frame prima che siano trascorsi 3 bit recessivi dal precedente (campo ITM), quindi la condizione rivendicata fa sì che il messaggio in corso e il messaggio di errore terminino nello stesso istante, in questo modo soddisfacendo automaticamente la condizione sull'allineamento[1].

Il problema tecnico dunque è come adattare la soluzione del documento D1 per avere una corretta gestione del bus CAN inserendo i bit di corruzione.

Non vi è nulla nel documento D1 o nell'arte che sia pertinente né al problema tecnico della corretta gestione del bus, cioè dei problemi generati dall'inserimento dei bit di corruzione, né a mezzi per mantenere l'allineamento, quindi ovviamente neppure allo ancora più specifico procedimento di inserimento rivendicato nella rivendicazione 1.

Dunque il tecnico del settore non avrebbe avuto alcun incentivo o indicazione per arrivare alle caratteristiche non descritte nel documento D1 e alla soluzione come rivendicata nella rivendicazione 1.

Dunque la rivendicazione 1 riveste un'altezza inventiva a fronte del documento D1 e dello stato dell'arte citato.

4.3 Riguardo alle rivendicazioni dipendenti, trattate in maniera molto sommaria dall'Esaminatore europea, si vuole aggiuntivamente sottolineare che a fronte dell'arte nota citata almeno due rivendicazioni, indicate senza spiegazione come meri dettagli implementativi, viceversa chiaramente si riferiscano a ulteriori aspetti che conferiscono di per sé novità e altezza inventiva.

La rivendicazione 4, relativa alla procedura di oscuramento riguarda una procedura per mascherare l'operazione di corruzione al nodo CAN che ha inviato il frame non lecito, evitando così la ritrasmissione automatica, con conseguente occupazione del CAN bus, da parte del nodo CAN malevolo. Il documento D1 è lontanissimo dall'insegnare una simile procedura, che ha un effetto e un vantaggio tanto marcati nel combattere i nodi malevoli, che quindi non si può certo riguardare come un dettaglio implementativo: viceversa riveste di per sé un'altezza inventiva.

Lo stesso si può affermare serenamente riguardo al contenuto della rivendicazione 7, dove la scelta della polarità (non praticata dalla soluzione descritta nel documento D1 che usa solo bit dominanti), fornisce una ulteriore certezza sull'allineamento, ottenuto secondo il procedimento di per sé inventivo della rivendicazione 1.

---

[1] Più in generale, per un messaggio in corso di trasmissione da parte di un nodo trasmittente A, se si ha uno stuff-error, allora i nodi riceventi inviano immediatamente un ERROR frame, cioè subito dopo la rilevazione dell'errore e quindi prima che la trasmissione in corso sia terminata. Ciò significa che, in assenza di ulteriori misure, il nodo trasmittente A diventerebbe consapevole che il suo messaggio non è stato correttamente ricevuto. Questo, in condizioni normali è corretto che accada, ma in presenza di un attaccante occorre mettere in atto una politica tale per cui il messaggio in corso da parte del nodo A trasmittente e l'ERROR frame inviato dai riceventi terminino esattamente nello stesso istante.

La misura prevista e rivendicata consiste nell'inserimento della corruzione di stuff-error in un momento specifico del campo CRC, cioè nel tempo di bit rivendicato nella rivendicazione 1.

5. In conclusione, è opinione della Richiedente, avendo provveduto a emendare le rivendicazioni introducendo materia indicata come nuova e inventiva nell'opinione di brevettabilità:

- che le anteriorità citate nel rapporto di ricerca non siano più da considerare rilevanti nei confronti dell'invenzione come ora rivendicata, e
- che le obiezioni espresse nell'opinione di brevettabilità allegata al rapporto di ricerca siano ora superate in vista degli emendamenti ora introdotti alle rivendicazioni.

* * *

Si confida che le modifiche apportate alla presente domanda possano portare al celere rilascio del brevetto.

Buzzi, Notaro & Antonielli d'Oulx

Giorgio Crovini

All.: - pagine 29-33 (rivendicazioni) con modifiche evidenziate
- pagine 29-33 (rivendicazioni) definitive

RIASSUNTO

Viene descritto un procedimento di protezione da attacchi informatici in una rete di comunicazione CAN (Controller Area Network) (20) di un veicolo comprendente un bus CAN (10) e una pluralità di nodi (11) associati a detto bus CAN (10) in rapporto di scambio di segnale e associati almeno in parte a unità di controllo di funzioni del veicolo,

comprendente le operazioni di

analizzare il contenuto di messaggi CAN (M) in transito fra nodi di detta pluralità di nodi (11) per identificare messaggi CAN non leciti (MF),

bloccare (B1, B2) detti messaggi non leciti (MF), detta operazione di bloccare (B1, B2) comprendendo di rendere non validi (F1, F2) detti messaggi non leciti (MF) rispetto a una verifica di integrità eseguita da un controllore CAN (13) di detti nodi (11), inserendo (F1) una sequenza di bit (NV) di corruzione riconosciuta come un errore da detto controllore CAN (13), ottenendo un messaggio corrotto (MF'). Secondo la soluzione qui descritta è previsto di inserire (F1) detta sequenza di bit (NV) di corruzione in un campo di controllo integrità (S5), in particolare un campo CRC, del messaggio CAN non lecito (MF) a un tempo di bit (bt_{j-5}) il cui valore è tale da allineare temporalmente un campo separatore (ITM) del messaggio non lecito con un corrispondente campo separatore di un messaggio d'errore (EM) generato da un nodo della rete (20) che riceve detto messaggio non lecito (MF) comprendente detta sequenza di corruzione (NV). Al fine di garantire l'allineamento dei campi separatore (ITM) del messaggio non lecito (MF) e il messaggio d'errore (EM), la

soluzione qui descritta prevede anche un'operazione di oscuramento (F2) atta a mascherare l'invio del/dei messaggio/i di errore (EM) e ad emulare la corretta ricezione (OR) del/dei messaggio/i non lecito/i.

(Figura 6)

DESCRIZIONE dell'invenzione industriale dal titolo:
"Procedimento di protezione da attacchi informatici al veicolo e corrispondente dispositivo"
di: Magneti Marelli S.p.A., nazionalità italiana, viale Aldo Borletti 61/63, 20011 Corbetta MI e Università di Pisa, Lungarno Antonio Pacinotti 43, 56126 Pisa PI.
Inventori designati: Christian ROSADINI, Walter NESCI, Luca BALDANZI, Luca CROCETTI, Luca FANUCCI
Depositata il: 31 dicembre 2018

***

TESTO DELLA DESCRIZIONE

La presente invenzione riguarda tecniche di protezione da attacchi informatici in una rete di comunicazione CAN (Controller Area Network) di un veicolo comprendente un bus CAN e una pluralità di nodi associati a detto bus CAN in rapporto di scambio di segnale e associati almeno in parte a unità di controllo di funzioni del veicolo,

comprendente le operazioni di

analizzare il contenuto di messaggi CAN in transito fra nodi di detta pluralità di nodi per identificare messaggi CAN non leciti,

bloccare detti messaggi non leciti,

detta operazione di bloccare comprendendo di rendere non validi detti messaggi non leciti rispetto a una verifica di integrità eseguita da un controllore CAN di detti nodi, inserendo una sequenza di bit di corruzione riconosciuta come un errore da detto controllore CAN, in particolare sostituendo parte della sequenza originale di bit con una di corruzione, ottenendo un messaggio corrotto.

Il bus CAN, adottato come BUS di comunicazione negli autoveicoli, è un mezzo di comunicazione di tipo seriale e multi-master, in cui ogni master, detto anche nodo connesso

al bus è in grado di inviare, ricevere e risolvere i conflitti di accesso contemporaneo in invio da parte di più nodi.

Un nodo 11 in grado di comunicare su bus CAN 10 comprende in generale, come mostrato in figura 1a:

- un ricetrasmettitore CAN, o CAN Transceiver, 12, associato attraverso a una linea di trasmissione TT e una linea di ricezione TR al CAN bus 10 e configurato per gestire i livelli elettrici propri del bus CAN (livello Fisico del modello OSI);
- un controllore CAN, o CAN Controller, 13, che è connesso attraverso rispettive linee di trasmissione CT e ricezione CR al ricetrasmettitore CAN 12, e configurato per gestire i livelli logici e la serializzazione del bus CAN 10 (livello Data link del modello OSI);
- un microcontrollore 14, che contiene la logica di invio e ricezione dei messaggi (gestione dei livelli OSI superiori al livello Data link).

In figura 1A è riportata una delle possibili soluzioni di implementazione che prevede che il controllore CAN 13 e il microcontrollore 14 siano posti in uno stesso System-on-Chip 15, mentre il ricetrasmettitore CAN è su un chip separato.

E’ noto installare un dispositivo di protezione 16 da attacchi informatici tra il controllore CAN 13 e il ricetrasmettitore CAN 12, come mostrato in Figura 1. Il dispositivo di protezione 16 elabora, in particolare analizza, i messaggi in transito tra il controllore CAN 13 e il ricetrasmettitore CAN 12 individuando i messaggi non leciti, o malevoli, e attua delle operazioni di bloccaggio dell’iniezione di tali messaggi malevoli su bus CAN in

differenti casi d'uso, che sono descritti nelle Figure 2, 3, 4 e 5.

In particolare, in figura 1B il dispositivo di protezione 16 riceve messaggi CAN sulla linea di trasmissione CT dal controllore CAN 13 al dispositivo di protezione 16, li analizza e li filtra, tramite le summenzionate operazioni di bloccaggio, sicché la linea fra dispositivo di protezione 16 e ricetrasmettitore CAN 12 è una linea di trasmissione filtrata DT su cui transitano i messaggi CAN elaborati dal dispositivo di protezione 16. Viceversa i messaggi CAN arrivano dal ricetrasmettitore 12 al dispositivo di protezione sulla linea di ricezione CR, che connette tali moduli, e sono elaborati al dispositivo di protezione 16 e trasmessi su una linea di ricezione filtrata DR al controllore CAN 12 dal dispositivo di protezione 16.

In particolare in Figura 2, è mostrato un caso in cui data una rete veicolare 20 che comprende una pluralità di nodi 11_1….11_n, rappresentativi ad esempi di centraline veicolari, quali ECU (Electronic Control Unit), ad esempio Engine Control Unit, ma anche centraline per l'illuminazione, il condizionamento, controllo trasmissione, ABS, controllo sospensioni, e altri moduli a processore dedicati altri servizi veicolari. In tale pluralità di nodi 11_1…11_n il nodo 11_1 è un nodo protetto, equipaggiato di dispositivo di protezione 16, ed è raffigurato il caso in cui tale nodo 11_1 protetto è malevolo e inietta messaggi CAN, o CAN frame, malevoli, cioè non leciti, MF verso la rete veicolare 20. Tale caso d'uso è quello in cui ad esempio il microcontrollore 14 è stato violato per mezzo di altri canali di comunicazione, come ad esempio un canale wireless, come può accadere per

nodi corrispondenti a unità di Infotainment/Telematics. In questo caso la presenza del dispositivo di protezione 16 evita che tali messaggi MF raggiungano la rete veicolare 20, ossia gli altri nodi non protetti 11_2….11_n.

In Figura 3 è mostrato il caso in cui i messaggi CAN malevoli MF sono iniettati dalla rete veicolare 20, ossia da uno dei nodi privi di dispositivo di protezione, ossia nodi non protetti, 11_2….11_n, in particolare il nodo 11_2. Tale figura rappresenta il caso d'uso in cui un nodo qualunque della rete veicolare 20 è stato violato. In questo caso la presenza del dispositivo di protezione 16 evita che i messaggi non pertinenti al rispettivo nodo CAN protetto 11_1 su cui è installato possano essere elaborati dal microcontrollore 14.

In Figura 4 è mostrato il caso in cui il dispositivo di protezione 16 è impiegato all'interno di un CAN gateway 18. Tale configurazione permette di isolare due reti CAN distinte 20A e 20B, con rispettivi nodi $11A_1$…$11A_n$ e $11B_1$…$11B_n$, in generale non protetti, di garantire il filtraggio dei frame CAN in transito da e tra una rete e l'altro. Nel caso specifico di figura 4, il dispositivo di protezione 16 blocca i messaggi non leciti MF trasmessi dalla rete 20A e ne impedisce la diffusione sulla rete 20B. E' chiaro che il dispositivo di protezione 16 può anche bloccare un messaggio CAN non lecito MF trasmesso da un nodo della rete 20B verso la rete 20A attraverso il gateway 18.

La domanda di brevetto statunitense US2015/191136 A1 descrive un dispositivo di protezione che opera in CAN bus di autoveicoli che prevede di bloccare messaggi in transito i cui parametri verificano criteri di messaggio non lecito. Il blocco è operato rendendo non validi rispetto a una

verifica di validità eseguita dal controllore CAN, ossia corrompendo, i messaggi non leciti durante la loro trasmissione fra il ricetrasmettitore CAN e il controllore CAN, inserendo una sequenza di bit riconosciuta come un errore dal controllore CAN, in particolare bit di stuffing, o bit di riempimento, in particolare inserendo uno Stuff error mediante una sequenza che non rispetta la regola del bit stuffing previsto dal protocollo CAN che determina da parte del dal controllore CAN di ignorare tali messaggi non leciti e non propagare tali messaggi non leciti sulla rete CAN. Tuttavia, la manipolazione del numero di stuff bit può generare un disallineamento temporale tra il messaggio corrotto (inviato sul bus) ed il messaggio "Error-Frame" generato dal nodo CAN che riceve il messaggio corrotto.

La presente invenzione si prefigge lo scopo di ottenere un procedimento di monitoraggio che permetta di rendere non validi i messaggi non leciti, operando un corretto allineamento.

Secondo la presente invenzione, tale scopo viene raggiunto grazie ad un procedimento di protezione nonché a un corrispondente dispositivo di protezione aventi le caratteristiche richiamate in modo specifico nelle rivendicazioni che seguono.

L'invenzione verrà descritta con riferimento ai disegni annessi, forniti a puro titolo di esempio non limitativo, in cui:

- le Figure 1A e 1B, 2, 3, 4 sono già state descritte in precedenza;

- la Figura 5 rappresenta uno schema di principio del dispositivo di protezione implementante il procedimento qui descritto;

- la Figura 6 è un diagramma che rappresenta

schematicamente messaggi CAN elaborati dal dispositivo di protezione;

- le Figure 7A, 7B, 7C rappresentano schematicamente il dispositivo di protezione qui descritto in tre fasi di funzionamento del procedimento;

- la Figura 8 è un diagramma di flusso che rappresenta operazioni del procedimento qui descritto.

In Figura 5 è riportato uno schema a blocchi di principio di un dispositivo di protezione 26 secondo l'invenzione. Tale dispositivo di protezione 26 è mostrato disposto fra un controllore CAN 13 e un ricetrasmettitore CAN 12 in un nodo protetto di una rete CAN 10, come ad esempio nella configurazione di figura 3 del nodo 11_1. La soluzione qui descritta prescinde dalla versione di CAN su cui è applicata (CAN2.0 e CAN-FD, quindi) e per semplicità di esposizione viene descritto solo lo scenario relativo alla versione CAN2.0

Il dispositivo di protezione 26 comprende un modulo di firewall 261, che in generale riceve una sequenza di messaggi CAN M inviati sulla linea di ricezione CR e sulla linea di trasmissione CT e invia una sequenza filtrata di messaggi CAN sulle linee filtrate di ricezione DR e trasmissione DT. I messaggi M possono essere, come detto, messaggi non leciti MF. La sequenza filtrata, come meglio descritto nel seguito, può contenere i messaggi CAN M medesimi, può contenere messaggi corrotti MF' ottenuti dai messaggi non leciti MF oppure può applicare il blocco tramite corruzione (modalità B2 descritta nel seguito) in modo totale ai messaggi M leciti e non leciti MF.

Dunque, tale modulo di firewall 261 è configurato per:

- estrarre il contenuto informativo di un messaggio CAN M transitante sulle linee di trasmissione CT o

ricezione CR;

- operare l'analisi di tale contenuto informativo. Ciò ad esempio comprende confrontare valori di campi del messaggio CAN M transitante con un insieme di regole di firewall R memorizzate in un modulo di immagazzinamento regole 262 che rappresenta una base dati di regole, cui il modulo di firewall 261 ha accesso almeno in lettura;
- rendere non valido il messaggio CAN M in transito, qualora identificato in base al contenuto come messaggio CAN non lecito MF. Ciò avviene operandone la corruzione durante la trasmissione dal dispositivo di protezione 26 in accordo a modalità di blocco, ad esempio B1 e B2, meglio dettagliate nel seguito, nel caso in cui il messaggio M analizzato sia identificato come messaggio non lecito MF, mentre tale messaggio non lecito MF è ancora in transito sul bus CAN;

Come detto, il dispositivo di protezione 26 comprende inoltre una base dati di regole 262, che è la base dati che contiene regole R applicate dal firewall 261 ai messaggi CAN analizzati, cioè in transito, per identificare messaggi non leciti MF. I messaggi CAN M in transito, in arrivo dalla linea di trasmissione CT e dalla linea di ricezione CR, possono essere assoggettati a un medesimo insieme di regole R nel database di regole 262 oppure tale database di regole 262 può contenere due insiemi di regole applicati indipendentemente alla ricezione CR e alla trasmissione CT.

Il dispositivo di protezione 26 comprende inoltre un modulo di memorizzazione operazioni 263, ossia un'area di memoria dedicata per memorizzare un registro, o "log", di operazioni B svolte dal dispositivo di protezione 26 sul bus CAN 10. Il dispositivo di protezione 26 accede a tale

modulo 263 per scrivere tali operazioni B svolte dal dispositivo di protezione sul bus CAN 10. Tale registro B comprende statistiche relative all'attività del firewall 261, quali quantità di frame non leciti MF corrotti sulla linea di trasmissione CT, quantità di frame non leciti corrotti sulla linea di ricezione CR, etc …) e che possono essere consultate mediante un'interfaccia di configurazione 264 che può accedere in lettura al modulo di memorizzazione operazioni 263 come indicato in figura 5.

Il dispositivo di protezione 26 comprende poi, come detto, una interfaccia di configurazione 264 per definire le regole R di filtraggio applicate dal firewall 261 e memorizzate nel modulo 262. In particolare tale interfaccia di configurazione può ricevere una configurazione di filtraggio, cioè le regole R, del dispositivo di protezione 26 da un'interfaccia di comunicazione esterna non mostrata in figura. Tale interfaccia di configurazione 264 è in rapporto di scambio di dati con la base dati di regole 262, nella quale scrive ad esempio l'insieme di regole R per il filtraggio tramite firewall ed il modulo di memorizzazione operazioni 263, come detto ad esempio per leggere i dati del log delle operazioni del firewall 261.

Associato all'interfaccia di configurazione 264 è un modulo di autenticazione 265, che è configurato per verificare l'autenticità della configurazione di filtraggio ricevuta dall'interfaccia di comunicazione esterna, ad esempio tramite meccanismi di firma digitale e cifratura dei dati.

Il dispositivo di protezione 26 è in generale configurato per implementare un filtro che blocchi i messaggi CAN malevoli e non pertinenti, lasciando passare solamente i dati leciti

La distinzione tra messaggi leciti e illeciti può essere configurata in base alla destinazione d'uso del dispositivo di protezione 26 e definita attraverso i seguenti parametri distintivi C:

C1: identificativo messaggio CAN;

C2: lunghezza del messaggio CAN;

C3: tempi di trasmissione, ad esempio una frequenza nel caso di messaggio periodico;

C4: contenuto del messaggio. Tale parametro è impiegato solo per i messaggi di tipo diagnostico;

C5: stato del veicolo. Tale parametro è impiegato solo per i messaggi di tipo diagnostico;

C6: percentuale di utilizzo del bus nell'unità di tempo.

Il dispositivo di protezione 26 è configurato per applicare l'insieme delle regole R in generale ai messaggi non diagnostici e diagnostici, applicando in tale insieme ulteriori e specifiche regole di filtraggio nel caso in cui sia riconosciuto in transito un frame di tipo diagnostico

Il dispositivo di protezione 26 è inoltre configurato, in particolare tramite il modulo firewall 261, per operare due modalità di blocco del messaggio:

una modalità di blocco selettiva B1: vengono bloccati tutti e soli i messaggi CAN MF non leciti

una modalità di blocco totale B2: tutti i messaggi CAN vengono bloccati, sia leciti M che non leciti MF.

La modalità di blocco totale B2 è configurabile nei seguenti modi d'impiego:

primo modo d'impiego BC1, in la modalità di blocco totale B2 è abilitata o disabilitata,

secondo modo d'impiego BC2, in cui se la modalità di blocco totale B2 è abilitata, è possibile definire

nel dispositivo di protezione 26 il tipo di violazione e il numero di violazioni, per ognuno dei tipi di violazione specificati, raggiunto il quale la modalità di blocco totale B2 deve essere attivata, nonché il tempo per cui deve rimanere attiva. Nel secondo modo d'impiego B2 si definiscono quindi uno o più parametri di disattivazione in una lista comprendente tipo di violazione, numero di violazione, tempo di disattivazione;

La modalità di blocco totale B2 permette di disconnettere virtualmente un i-esimo nodo 11_i o una rete (es. 20B in figura 4) dal bus CAN 10 per un periodo di tempo arbitrario che, in base alla configurazione, può anche essere pressoché perpetuo, isolando quindi completamente il nodo 11_i o rete oppure ripristinando le capacità di comunicazione del nodo 11_i al termine del periodo di tempo impostato.

Il meccanismo mediante il quale il dispositivo di protezione 26 blocca un messaggio CAN non lecito implementa una modalità a zero-ritardo. Ciò rende vantaggioso l'utilizzo del dispositivo di protezione 26 in tutte le applicazioni in cui i ritardi di propagazione introdotti da elementi filtranti aggiuntivi, come appunto è il dispositivo di protezione 26, devono essere minimizzati.

Come detto, la modalità di filtraggio dei messaggi a zero-ritardo, implementata dal dispositivo di protezione 26, prevede di sfruttare i meccanismi di controllo integrità di per sé presenti nel bus CAN, rendendo non valido, cioè corrompendo, il messaggio CAN non lecito MF durante la trasmissione sul bus CAN, in modo tale che i nodi riceventi ignorino il suddetto messaggio non lecito MF già a livello digitale di controllore CAN 13, ossia il

livello Data link, ove viene effettuato il controllo di integrità del messaggio, senza andare a propagare il messaggio al microcontrollore 14 (e ai livelli superiori dello stack OSI). Pertanto, tale modalità a zero ritardo si contrappone a quella in cui l'elemento filtrante riceve-analizza-ritrasmette, come è tipico comportamento dei gateway, in quanto anche nella condizione ideale di tempi di analisi nullo, l'elemento filtrante deve comunque attendere che il messaggio termini prima di poterlo analizzare e, nel caso sia lecito e debba essere ritrasmesso, partecipare nuovamente alla fase di contesa e arbitraggio del bus (dopo la fase di analisi), introducendo un ritardo aggiuntivo pari ad almeno la durata della ritrasmissione del messaggio stesso. Inoltre, poiché è necessario che l'elemento filtrante vinca la contesa del bus CAN affinché possa procedere alla ritrasmissione del messaggio precedentemente analizzato, tale ritardo aggiuntivo può risultare essere significativamente più lungo, con un limite superiore, a causa delle caratteristiche del protocollo CAN, teoricamente infinito: caso di trasmissione di messaggi con priorità superiore da parte di altri nodi della rete.

La modalità a zero-ritardo implementata dal dispositivo di protezione 26 invece, permette di ispezionare un messaggio CAN in transito, cioè durante la trasmissione o la ricezione stessa da parte del nodo su cui è installato, e consente quindi:

- di agire prontamente corrompendo il messaggio non lecito prima ancora che la sua trasmissione o ricezione termini
- lasciar passare il messaggio inalterato se lecito, non impattando quindi il suo tempo di propagazione.

La procedura di filtraggio del frame CAN a zero ritardo, tramite la prima modalità di blocco selettivo B1 o seconda modalità di blocco totale B2, implementata dal dispositivo di protezione 26, comprende specificamente due operazioni che determinano che il tempo di propagazione del messaggio CAN non sia alterato e che il messaggio non lecito sia ritenuto, dal nodo malevolo, inviato con successo.

Una prima operazione è un'operazione F1 di blocco del messaggio in transito al dispositivo di protezione 26 tramite corruzione della sequenza di bit del messaggio CAN stesso.

Una seconda operazione è un'operazione F2 di oscuramento al nodo CAN malevolo che trasmette il messaggio CAN MF non lecito intercettato dal dispositivo di protezione 26 della corruzione di tale messaggio CAN non lecito da lui trasmesso, e quindi del suo conseguente bloccaggio da parte dei controlli d'integrità nei controllori CAN degli altri nodi CAN.

In conseguenza di tali modalità di blocco B1 o B2 tramite corruzione F1 e di oscuramento F2, il dispositivo di protezione 26 e il procedimento di protezione implementato da tale dispositivo 26 permettono di garantire la simultaneità tra la fine del transito del messaggio CAN non lecito, e corrotto tramite l'operazione F1 da parte del dispositivo di protezione 26, e la fine della trasmissione di un messaggio di errore in risposta a tale messaggio CAN non lecito corrotto, ossia come conseguenza derivante dalla rilevazione della condizione di errore introdotta dal dispositivo di protezione 26 nel messaggio CAN malevolo, al fine di corromperlo, da parte del/dei nodo/nodi CAN ricevente/i, $11_1 \ldots 11_n$, diversi dal nodo che comprende il

dispositivo di protezione 26 che applica l'operazione di blocco F1 al messaggio non lecito MF e diversi dal nodo CAN che inietta il messaggio malevolo MF.

Tale simultaneità rappresenta un aspetto fondamentale al fine di impedire l'innesco di sovrapposizioni non allineate di invio di messaggi che porterebbero a continue corruzioni dei dati sul bus CAN 10, con overhead sulla occupazione del bus, e, da ultimo, ad una interruzione della comunicazione.

Il procedimento di protezione implementato dal dispositivo di protezione tramite le operazioni di corruzione F1 e oscuramento F2 sfrutta la particolare struttura dei messaggi di tipo Dato ed Errore del protocollo CAN; in particolare il messaggio di tipo Dato è strutturato con sezioni S di bit contigue elencate di seguito nella tabella 1:

	Sezione S [dimensione in bit]	Contenuto sezione S
S1	SOF [1 bit]	inizio messaggio CAN
S2	Arbitration Field [12/32 bit]	contiene identificativo messaggio
S3	Control Field [6 bit]	contiene l'informazione della lunghezza dei dati trasmessi
S4	Data Field [0÷64 bit]	sezione dati (contenuto informativo del messaggio)
S5	CRC Field [16 bit]	codice per controllo integrità

		(con campo di delimiter)
S6	ACK Field [2 bit]	per conferma ricezione corretta da parte degli altri nodi (con campo di delimiter)
S7	EoF [7 bit]	zona di bit recessivi necessaria per segnalare la fine messaggio
S8	ITM [3 bit]	zona di bit recessivi che funge da separatore tra messaggi

Tabella 1

La struttura delle sezioni S del messaggio di tipo Dato è naturalmente di per sé nota, nello standard del bus CAN.

I messaggi di tipo Errore comprendono messaggi di tipo Attivo e Passivo strutturati come in Tabella 2 per l'Errore Attivo:

	Sezione S [dimensione in bit]	Contenuto sezione S
SE1	Active Error Flag[6 bit]	bit dominanti
SE2	Error delimiter[8 bit]	Campo che segnala la fine del messaggio di errore
SE3	ITM [3 bit]	zona di bit recessivi che funge da separatore

		tra messaggi

Tabella 2

mentre sono strutturati come in Tabella 3 per l'Errore Passivo:

	Sezione S [dimensione in bit]	Contenuto sezione S
SP1	Passive Error Flag[6 bit]	bit recessivi
SP2	Error delimiter[8 bit]	Campo che segnala la fine del messaggio di errore
SP3	ITM [3 bit]	zona di bit recessivi che funge da separatore tra messaggi

Tabella 3

In Figura 6, a titolo di esempio, viene mostrato un caso riferito all'Errore Attivo. Con MF è indicato il messaggio CAN non lecito in trasmissione, mentre con MF' è indicato il messaggio corrotto contenente in coda un messaggio d'errore EM, un messaggio CAN di tipo Errore in Risposta, da uno dei nodi riceventi, dopo che il controllo integrità del suo controllore CAN rileva la corruzione.

Con bt è indicato inoltre un'asse del tempo di bit e con NV un segnale scritto dal dispositivo di protezione 26 nel messaggio CAN non lecito MF. Con S_i è indicato il segnale interno generato dal dispositivo di protezione. In particolare il segnale S_i è il segnale DT nel dispositivo di protezione 26 nel caso di messaggio in trasmissione, o alternativamente è il segnale DR del dispositivo di protezione 26 nel caso di messaggio in ricezione.

Affinché sia garantita la simultaneità della fine della trasmissione del messaggio CAN non lecito MF, di tipo Data, corrotto dal dispositivo di protezione 26, e il

relativo messaggio EM di tipo Errore di risposta, emesso da parte di uno qualsiasi dei nodo riceventi 11, ovvero affinché i campi ITM (campo S8 per il messaggio non lecito MF e campo SE3 per il messaggio di errore EM) di tali messaggi siano allineati e sovrapposti, è necessario inserire una condizione di errore in un punto esatto, ossia ad uno specifico valore di bit time bt del messaggio non lecito MF. Ciò viene eseguito in particolare sostituendo parte della sequenza originale di bit con una di corruzione, ottenendo un messaggio corrotto.

Il punto esatto in cui effettuare l'inserimento della sequenza di corruzione di 6 bit consecutivi (NV) è univocamente determinato dal formato del pacchetto e dalle regole del protocollo CAN e richiede l'impiego di risorse/moduli logici dedicati al computo dello stesso e al computo della polarità dei bit che costituiscono detta sequenza di corruzione NV.

In particolare, per calcolare il punto di inizio della sequenza di 6 bit consecutivi all'interno del campo CRC e la polarità (dominante o recessiva) dei bit che la compongono, il dispositivo di protezione 26, in particolare il modulo di firewall 261, è dotato di uno o più moduli/elementi logici atti a o configurati per:

- calcolare dinamicamente (a runtime) il valore del campo CRC (Cyclic Redundancy Check) S5 al fine di prevedere il numero di stuff bit che saranno presenti all'interno del campo CRC;
- analizzare il contenuto del campo CRC ricostruito nel passo precedente tenendo conto anche dei bit che precedono il CRC, al fine di valutare il numero di stuff bit che saranno presenti nel campo CRC, ossia nel campo S5 del messaggio M, MF. Poiché il campo CRC

è data-dependent (e quindi varia a runtime così come i dati) anche il punto di inserzione esatto della sequenza di corruzione è determinato in modo dinamico.

Con riferimento alla figura 6, il punto esatto di inserzione nella sequenza di corruzione è l'istante bt_{j-5}, mentre l'istante in cui il nodo ricevente rileva la condizione di "Stuff error" (SPE) è l'istante bt_j. Con bt_{j-6} è indicato l'ultimo bit immediatamente precedente al primo bit della sequenza di corruzione, al fine di sottolineare che la sequenza di corruzione deve avere polarità opposta a tale bit.

In conseguenza di ciò:

- il nodo CAN 11 che riceve il messaggio MF corrotto risponde con un messaggio di errore EM (campi SE1, SE2, SE3 in quanto nell'esempio è illustrato un Errore Attivo, diversamente si impiegano i campi SP1, SP2, SP3 dell'Errore Passivo) a partire dal bit time bt_{j+1} immediatamente successivo a quello bt_j nel punto in cui si verifica la condizione di Stuff error SPE. Più specificamente, come mostrato nella figura 6, a partire dal bit time bt_{j+1} viene scritto il messaggio d'errore EM. Nel caso di più nodi riceventi, ciascun nodo ricevente 11_i trasmette un messaggio CAN EM di tipo Errore i cui frame d'errore sono esattamente sovrapposti a quelli di qualsiasi altro messaggio CAN EM di tipo Errore inviato da qualsiasi altro nodo ricevente;

- il termine del messaggio (o dei messaggi sovrapposti) di Errore, il campo SE3 ITM, che contiene una zona di bit recessivi, specificamente 3 bit, che funge da separatore tra messaggi è allineato temporalmente con il corrispondente campo ITM, S8, del messaggio non lecito MF, che è contemporaneamente ritrasmesso inalterato al nodo

malevolo mittente.

Anche a parità di lunghezza dei vari campi del frame di tipo Data di un messaggio CAN, la lunghezza del messaggio CAN può variare in base al loro contenuto, a causa della eventuale inserzione di bit di stuffing o bit di riempimento, pertanto il dispositivo di protezione 26 è configurato per calcolare dinamicamente, messaggio CAN per messaggio CAN, il punto di inserzione bt_{j-5} del campo CRC in cui è necessario inserire la sequenza NV di 6 bit consecutivi con la stessa polarità, nel caso in cui il frame MF debba essere corrotto. Il dispositivo di protezione 26 è configurato per calcolare dinamicamente, messaggio CAN per messaggio CAN, sia il punto di inserzione bt_{j-5} del campo CRC in cui è necessario inserire la sequenza NV di 6 bit consecutivi con la stessa polarità, sia la polarità dei bit di suddetta sequenza NV, la quale deve essere opposta a quella del bit bt_{j-6}, nel caso in cui il frame MF debba essere corrotto.

Come detto l'altra operazione fondamentale eseguita dal dispositivo di protezione 26 è l'oscuramento F2 al nodo CAN malevolo che trasmette il messaggio CAN non lecito intercettato dal dispositivo di protezione 26 della corruzione di tale messaggio CAN non lecito da lui stesso trasmesso, e quindi del suo conseguente blocco da parte dei controlli d'integrità nei controllori CAN degli altri nodi CAN.

Nel caso in cui il dispositivo di protezione 26 corrompa un frame non lecito MF, se il dispositivo di protezione 26 non nascondesse la corruzione, (ovvero la sequenza NV inserita in un punto di inserzione bt_{j-5} del campo CRC S5 del frame non lecito MF e la quale determina la condizione di Stuff error SPE al punto bt_j), il nodo CAN

mittente del frame malevolo MF rivelerebbe tale condizione di Stuff error SPE e, come conseguenza, procederebbe alla interruzione della trasmissione del frame malevolo MF, alla trasmissione di un frame di tipo Errore EM (disallineato rispetto a tutti gli altri frame di tipo Errore inviati da tutti gli altri nodi riceventi) e successivamente tenterebbe di ritrasmettere il medesimo frame malevolo.

L'operazione di oscuramento F2 del processo di corruzione del messaggio in transito è gestita come illustrato in Figura 7, dove gli elementi "CAN Controller" 13 e "CAN Transceiver" 12 evidenziati sono quelli ad esempio appartenenti al nodo CAN protetto 11_1 su cui è installato il dispositivo di protezione 26 e tale nodo CAN protetto trasmette un messaggio malevolo MF (caso in cui lo host del nodo CAN su cui è installato il dispositivo di protezione 26 è stato violato). In particolare, poiché ogni bit del messaggio CAN MF trasmesso sulla linea di trasmissione CT viene anche riletto sulla linea di ricezione CR, il dispositivo di protezione 26 opera come segue, eseguendo l'operazione di corruzione, dopo che, come rappresentato in figura 7A, è stato individuato il frame malevolo MF in arrivo al dispositivo 26 sulla linea di trasmissione CT, del frame malevolo, in due fasi:

in una prima fase, rappresentata in figura 7B, dal lato host, ossia verso il nodo malevolo, (linee di trasmissione CT e di ricezione filtrata DR), il messaggio CAN non lecito MF è replicato senza alcuna alterazione del bitstream sulla linea di ricezione filtrata DR, mentre dal lato CAN bus a valle del ricetrasmettitore 12, ossia verso nodi riceventi non malevoli, ossia sulla linea di trasmissione filtrata DT e sulla linea di ricezione non filtrata CR, il messaggio non lecito MF viene corrotto in

maniera opportuna modificandone il bitstream, come messaggio corrotto MF';

in una seconda fase, rappresentata in figura 7C, dal lato host, ossia verso il nodo malevolo, il dispositivo di protezione 26 emula il bus CAN segnalando la corretta ricezione del messaggio da parte degli altri nodi $11_2 \ldots 11_n$ della rete 20, tramite un messaggio di corretta ricezione OR sulla linea di DR (figura 7C), in particolare tramite l'invio del bit dominante durante il bit time ACK Slot; contemporaneamente, dal lato CAN bus, il dispositivo di protezione 26 blocca la segnalazione di errore, tramite Error Frame EM previsto dal protocollo CAN, sulla linea CR ad opera degli altri nodi 11 della rete che hanno ricevuto il messaggio corrotto MF'.

L'operazione di oscuramento F2 del processo di corruzione del messaggio in transito si applica anche al caso di messaggio non lecito in ricezione, ovvero trasmesso da un nodo CAN 11_1, diverso dal nodo CAN protetto 11_1 su cui è installato il dispositivo di protezione 26, in maniera analoga a quanto sopra espresso e da quanto riportato dalle figure 7A, 7B e 7C, in conformità alle caratteristiche del protocollo CAN in caso di ricezione di messaggio. In particolare, il messaggio MF da replicare verso il nodo malevolo, che dovrebbe essere per dualità trasmesso su DT in questo caso non è necessario, ossia non si adotta nessuna azione di replica, ma è sufficiente un messaggio di corretta ricezione OR a testimonianza di corretta ricezione del messaggio malevolo (che questa volta è sul CAN bus 10).

Dunque, il procedimento di protezione da attacchi informatici in una rete di comunicazione CAN (Controller Area Network) 20 di un veicolo comprendente un bus CAN 10 e

una pluralità di nodi 11 associati a detto bus CAN 10 in rapporto di scambio di segnale e associati almeno in parte a unità di controllo di funzioni del veicolo, comprendente le operazioni di analizzare il contenuto di messaggi CAN M in transito fra nodi di detta pluralità di nodi 11 per identificare messaggi CAN non leciti MF, e bloccare tramite le modalità B1, B2 detti messaggi non leciti MF, dove tale operazione di bloccare tramite le modalità B1, B2 comprende di rendere non validi i messaggi non leciti MF, ossia corrompere F1, rispetto a una verifica di integrità eseguita da un controllore CAN 13, di detti nodi 11, inserendo F1 una sequenza di bit NV di corruzione riconosciuta come un errore da detto controllore CAN 13, ottenendo un messaggio corrotto MF', prevede specificamente di inserire F1 detta sequenza di bit NV di corruzione in un campo di controllo integrità S5, in particolare un campo CRC, del messaggio CAN non lecito MF a un tempo di bit bt_{j-5} il cui valore è tale da allineare temporalmente un campo separatore, ossia ITM, del messaggio non lecito con un corrispondente campo separatore di un messaggio d'errore EM generato da un nodo della rete 20 che riceve detto messaggio non lecito MF comprendente detta sequenza di corruzione NV. Si noti che tale operazione di inserire è effettuata sostituendo parte della sequenza originale di bit, in particolare del campo di controllo integrità S5, con una di corruzione, la sequenza di bit NV, in particolare tale sequenza di bit NV avendo polarità opposta alla polarità del bit al tempo bt_{j-6} precedente il bit al punto di inserzione bt_{j-5}, ottenendo un messaggio corrotto o non lecito MF.

Il procedimento descritto comprende poi di

estrarre un contenuto informativo del messaggio M in transito durante la trasmissione;

- operare l'analisi di detto contenuto informativo detto contenuto informativo in base a un insieme di regole di firewall (R),

- rendere non valido F1 il messaggio M qualora detta analisi del contenuto informativo identifichi il messaggio (M) analizzato come messaggio non lecito MF ottenendo un messaggio corrotto MF'.

Il procedimento descritto comprende poi di selezionare se applicare l'operazione di rendere non valido F1 il messaggio non lecito MF almeno secondo una modalità di blocco selettiva B1 a tutti e soli i messaggi CAN MF non leciti o secondo una modalità di blocco totale B2 a tutti i messaggi CAN, leciti M e non leciti MF.

Il procedimento descritto comprende poi che detta operazione di rendere non valido il messaggio non lecito MF comprenda un'operazione di oscurare F2 al nodo CAN o rete CAN che trasmette il messaggio CAN MF non lecito detta operazione di inserzione di bit NV di corruzione, tramite i passi di

replicare detto messaggio CAN non lecito MF senza alcuna alterazione, in particolare senza sequenza NV, verso il nodo CAN 11 che trasmette detto messaggio non lecito MF, oppure non adottare nessuna azione di replica verso la rete CAN 10 che trasmette detto messaggio non lecito MF,

emulare il bus CAN 10 oppure il nodo CAN 11 per il caso di trasmissione del messaggio non lecito da parte di CAN 11 o bus CAN 10, rispettivamente segnalando la corretta ricezione del messaggio non lecito MF da parte di un nodo ricevente o nodi riceventi e contemporaneamente bloccare messaggi di errore EM associati a detto messaggio non

lecito MF a detto nodo CAN o rete CAN che trasmette detto messaggio non lecito.

Tali operazioni sono implementate dal dispositivo di protezione 26, in particolare dal suo modulo di firewall 261 in base alle regole R memorizzate nel modulo di memorizzazione 262.

Il dispositivo di protezione 26 a questo scopo può essere in forme varianti è disposto fra un controllore CAN 13 e un ricetrasmettitore CAN 12 di un nodo CAN, che è così un nodo protetto, anche dovesse essere il medesimo nodo malizioso.

Il dispositivo di protezione 26 può essere in ulteriori forme varianti disposto interposto fra due reti CAN 20A, 20B in associazione a un gateway 18.

Il dispositivo di protezione 26 dispone come detto di una interfaccia di configurazione, l'interfaccia 264 che consente la definizione delle regole R di firewall tramite le seguenti liste e parametri:

- "white-list", ossia lista di elementi abilitati o ammessi, per i messaggi ammessi (per ciascuna direzione) da applicare in determinate condizioni veicolo. Ogni voce di questa lista comprende i seguenti campi:
  a) identificativo;
  b) lunghezza;
  c) parametri di trasmissione e di soglia di violazione;
  d) Tipo di messaggio (diagnostico/non-diagnostico)
- "white-list dei servizi diagnostici" ammessi (applicabile solo ai messaggi di tipo diagnostico);
- "black-list, ossia lista di elementi non abilitati o non ammessi, dei servizi diagnostici" non ammessi

(applicabile solo ai messaggi di tipo diagnostico) da applicare in determinate condizioni veicolo;

- "soglie di violazioni delle white/black list" per attivare la modalità di blocco totale;
- "soglie di occupazione del bus" per attivare la modalità di blocco totale;

"informazioni di rilevamento condizione veicolo" per determinare quale sia lo stato (ad es. velocità attuale maggiore di 5km/h) da usare congiuntamente alla "black-list dei servizi diagnostici" e alla "white list" dei messaggi ammessi.

Le regole di firewall R impostate mediante i parametri e le liste sopra riportate sono immagazzinate nelle tabelle del modulo di memorizzazione 262 e possono essere aggiornate aggiungendo nuove regole di firewall R oppure sovrascrivendo e/o eliminando le esistenti regole di firewall R. Il dispositivo di protezione 26 nel modulo di memorizzazione 263 memorizza tutte le informazioni B statistiche relative all'attività del firewall (quantità di frame non leciti corrotti sulla linea DT, quantità di frame non leciti corrotti sulla linea DR, etc …) e che possono essere consultate mediante l'interfaccia di configurazione 264 che può accedere al modulo 263 come indicato in figura 5.

L'applicazione delle regole di firewall R definite e contenute nel modulo di memorizzazione 262 è attuata per ogni messaggio CAN M di tipo Data frame o Remote frame. Una rappresentazione schematica del processo di filtraggio è rappresentata in Figura 8.

In accordo con il diagramma di flusso di figura 8, è descritta una forma realizzativa d'esempio di procedura di protezione 100 eseguita dal dispositivo di protezione 26.

Dopo un avvio 105 della procedura, in un passo 110 dal campo Arbitration S2 del messaggio CAN in transito M il firewall 261 estrae un identificativo messaggio (ID 11 / 29 bit), che viene confrontato con il relativo campo della "white-list" per la condizione del veicolo impostata. Se tale identificativo messaggio è presente si procede con il passo successivo 120, altrimenti il messaggio M viene considerato non lecito MF e si procede con il passo 180.

Al passo 120 dal campo Control S3 del messaggio CAN in transito M il firewall 261 estrae una lunghezza messaggio (DLC 4 bit), che viene confrontata con il relativo campo della "white-list". Se la lunghezza è corretta si procede con il passo successivo 130, altrimenti il messaggio CAN M viene considerato messaggio non lecito MF e si procede con il passo 180.

Al passo 130 viene misurato il tempo intercorso dall'ultima ricezione dello stesso messaggio, in base all'identificativo, e viene confrontato con delle soglie di temporizzazione configurate (ad esempio un intervallo di tempo definito fra un tempo massimo Tmax e uno minimo Tmin, o tramite un periodo etc, anche in relazione alla cronologia delle violazioni delle regole di temporizzazione. Se il tempo intercorso dall'ultima ricezione dello stesso messaggio risulta ricadere in un intervallo ammesso oppure non è nell''intervallo ammesso, ma il numero di violazioni rilevate è inferiore a un valore di soglia definita (parametri tutti estratti dalla "white list", come quelli di intervallo di tempo) si procede con il passo successivo 135 altrimenti il messaggio CAN M viene considerato messaggio non lecito MF e si procede con il passo 180.

In tale passo 135 viene verificato se il messaggio M è

di tipo diagnostico. In caso negativo si passa a un passo 160 di aggiornamento dello stato del veicolo. In caso affermativo, dal campo *Data* in un passo 140 viene estratto il valore del servizio diagnostico e controllato che sia presente nella "white-list dei servizi diagnostici" memorizzata nel modulo 262. Se presente si procede con il passo successivo 150 altrimenti il messaggio CAN M viene considerato messaggio non lecito MF e si procede con il passo 180.

Successivamente, nel passo 150 dal campo Data S4 viene estratto il valore del servizio diagnostico e controllato che non sia presente nella "black-list dei servizi diagnostici" per la condizione del veicolo impostata (si veda passo 160). Se presente il messaggio M viene considerato messaggio non lecito MF passando al passo 180, altrimenti lecito e si passa al passo 160 di aggiornamento dello stato del veicolo.

In tale passo 160, impiegando "informazioni di rilevamento condizione veicolo" congiuntamente ai campi di *Arbitration* e *Data del messaggio M* viene aggiornata l'informazione interna che rappresenta la condizione del veicolo. Specificamente, il passo 160 verifica se è necessario effettuare l'aggiornamento dello stato del veicolo. Il fattore discriminante per valutare se deve essere aggiornato lo stato del veicolo è contenuta nell'insieme delle regole R. La verifica si basa sui campi Arbitration e Data del frame in transito.

Quindi, in un passo 170, dalla lunghezza totale del messaggio viene aggiornato il valore dell'occupazione del bus e confrontato con le "soglie di occupazione del bus". Se il messaggio non rispetta tali soglie il messaggio CAN M viene considerato messaggio non lecito MF e si procede con

il passo 180. Viceversa la procedura 100 in un passo 195 ha termine.

Dunque, in generale, le operazioni del firewall 261 di estrarre il contenuto informativo di un messaggio CAN M transitante sulle linee di trasmissione CT o ricezione CR e operare l'analisi di tale contenuto informativo, comprendono una o più delle operazioni 110, 120, 130, 135, 140, 150, 170.

Nel passo 180, poiché il messaggio CAN M è considerato messaggio non lecito MF, viene determinato, combinando il tipo di violazione rilevata con le "soglie di violazioni delle white/black list" viene determinato se attivare la modalità di blocco B1 o B2.

Nel passo 190, le informazioni di validità del messaggio e della modalità di blocco B1 o B2 da attuare vengono trasmesse al blocco 261 di firewall che provvede a eseguire le operazioni richieste dalla modalità di blocco, ossia blocco totale (B1) oppure operazione di blocco tramite corruzione F1 e di oscuramento F2 (B2).

Il dispositivo di protezione 26 prevede di operare sia con messaggi diagnostici single-frame sia con messaggi multi-frame. Nel caso di messaggi diagnostici multi-frame, se viene riconosciuto come malevolo il primo frame della catena di messaggi, il dispositivo di protezione 26 è in grado di bloccare tale messaggio e tutti i messaggi successivi che compongono il messaggio multi-frame, attraverso il passo 135. Di conseguenza, sono presenti all'interno del dispositivo di protezione 26 contatori per tenere traccia di quanti CAN frame sono transitati sul CAN bus, e determinare quando terminare il processo di corruzione per uno specifico servizio diagnostico.

Dunque, da quanto descritto sopra, sono chiari i vantaggi della soluzione proposta.

Il dispositivo e procedimento descritti permettono di evitare il disallineamento temporale tra il messaggio corrotto (inviato sul bus) ed il messaggio "Error-Frame" generato dal nodo CAN che riceve il messaggio corrotto.

Il dispositivo e il procedimento descritti permettono inoltre, mediante un opportuno processo di offuscamento, di mascherare l'operazione di corruzione al nodo CAN che ha inviato il frame non lecito. In questo modo si evita la ritrasmissione automatica, con conseguente occupazione del CAN bus, da parte del nodo CAN malevolo.

Il dispositivo e procedimento descritti permettono di non introdurre alcun ritardo di propagazione dei messaggi CAN garantendone l'utilizzo in modo trasparente da parte dei nodi CAN coinvolti.

Il dispositivo e il procedimento descritti permettono di operare anche con i messaggi CAN di tipo diagnostico. Grazie ad una logica di controllo dedicata si è in grado di riconoscere una sequenza di messaggi diagnostici di tipo multi-frame ed invalidare, se il servizio diagnostico è identificato come malevolo, tutta la catena di messaggi.

RIVENDICAZIONI

1. Procedimento di protezione da attacchi informatici in una rete di comunicazione CAN, Controller Area Network, (20) di un veicolo comprendente un bus CAN (10) e una pluralità di nodi (11) associati a detto bus CAN (10) in rapporto di scambio di segnale e associati almeno in parte a unità di controllo di funzioni del veicolo,

comprendente le operazioni di

analizzare il contenuto di messaggi CAN (M) in transito fra nodi di detta pluralità di nodi (11) per identificare messaggi CAN non leciti (MF),

bloccare (B1, B2) detti messaggi non leciti (MF),

detta operazione di bloccare (B1, B2) comprendendo di rendere non validi (F1, F2) detti messaggi non leciti (MF) rispetto a una verifica di integrità eseguita da un controllore CAN (13) di detti nodi (11), inserendo (F1) una sequenza di bit (NV) di corruzione riconosciuta come un errore da detto controllore CAN (13), ottenendo un messaggio corrotto (MF'),

caratterizzato dal fatto di

inserire (F1) detta sequenza di bit (NV) di corruzione in un campo di controllo integrità (S5) del messaggio CAN non lecito (MF) a un tempo di bit (bt_{j-5}) il cui valore è tale da allineare temporalmente un campo separatore (ITM), comprendente una zona di bit recessivi che funge da separatore tra messaggi, del messaggio non lecito con un corrispondente campo separatore di un messaggio d'errore (EM) generato da un nodo della rete (20) che riceve detto messaggio non lecito (MF) comprendente detta sequenza di corruzione (NV).

2. Procedimento secondo la rivendicazione 1, caratterizzato dal fatto che comprende di

estrarre un contenuto informativo del messaggio (M) in transito durante la trasmissione;

– operare l'analisi di detto contenuto informativo detto contenuto informativo in base a un insieme di regole di firewall (R),

– rendere non valido (F1, F2, 190) detto messaggio (M) qualora detta analisi del contenuto informativo identifichi il messaggio (M) analizzato come messaggio non lecito (MF) ottenendo un messaggio corrotto (MF').

3. Procedimento secondo la rivendicazione 1, caratterizzato dal fatto di selezionare (180) se applicare detto operazione di rendere non valido (F1, F2, 190) il messaggio non lecito (MF) almeno secondo una modalità di blocco selettiva (B1) a tutti e soli i messaggi CAN (MF) non leciti o secondo una modalità di blocco totale (B2) a tutti i messaggi CAN (M, MF).

4. Procedimento secondo una delle rivendicazioni da 1 a 3, caratterizzato dal fatto che detta operazione di rendere non valido (F1, F2, 190) detto messaggio (MF) non lecito comprende un'operazione di oscurare (F2) al nodo CAN (11) o rete CAN (10) che trasmette il messaggio CAN (MF) non lecito detta operazione di inserzione di una sequenza di bit (NV) di corruzione, tramite i passi di

replicare detto messaggio CAN non lecito (MF) senza alcuna alterazione verso il nodo CAN (11) che trasmette detto messaggio non lecito (MF) oppure non adottare nessuna azione di replica verso la rete CAN (10) che trasmette detto messaggio non lecito (MF),

emulare il bus CAN (10) oppure il nodo CAN (11) per il caso di trasmissione del messaggio non lecito da parte di

CAN (11) o rete CAN (10), rispettivamente segnalando la corretta ricezione del messaggio non lecito (MF) da parte di un nodo ricevente o nodi riceventi e contemporaneamente bloccare messaggi di errore (EM) associati a detto messaggio non lecito (MF) a detto nodo CAN (11) o rete CAN (10) che trasmette detto messaggio non lecito (MF).

5. Procedimento secondo una delle rivendicazioni da 2 a 4, caratterizzato dal fatto che detto insieme di regole (R) di firewall comprende uno o più dei seguenti liste e parametri:

- white-list per i messaggi ammessi da applicare in determinate condizioni veicolo;
- white-list dei servizi diagnostici ammessi;
- black-list dei servizi diagnostici non ammessi da applicare in determinate condizioni veicolo;
- soglie di violazioni delle white list e black list per attivare la modalità di blocco totale (B2);
- soglie di occupazione del CAN bus (10) per attivare la modalità di blocco totale (B2);
- informazioni di rilevamento condizione veicolo indicative delle condizioni veicolo da impiegare per valutare detta black-list dei servizi diagnostici e detta "white list" dei messaggi ammessi.

6. Procedimento di protezione secondo la rivendicazione 5, caratterizzato dal fatto che comprende una o più delle seguenti operazioni di analisi del contenuto informativo del messaggio CAN (M)

– estrarre (110) un identificativo messaggio e confrontare con un campo corrispondente di una white-list per una data condizione del veicolo;

– estrarre (120) una lunghezza messaggio che viene confrontata con un campo corrispondente di un white list,

con il relativo campo della white-list

- misurato (130) di un tempo intercorso dall'ultima ricezione dello stesso messaggio e confronto con soglie di temporizzazione
    a) verifica, se il messaggio è di tipo diagnostico, della presenza in una white-list dei servizi diagnostici
    b) estrazione, se il messaggio è di tipo diagnostico, del valore del servizio diagnostico e verifica della presenza in una "black-list dei servizi diagnostici" per una data condizione del veicolo.
- verifica di un valore dell'occupazione del bus e confronto con delle soglie di occupazione del bus.

7. Procedimento di protezione secondo una delle rivendicazioni precedenti, caratterizzato dal fatto che l'ultimo bit (bt_{j-6}) immediatamente precedente al primo bit (bt_{j-5}) della sequenza di corruzione (NV) ha polarità opposta rispetto a detto primo bit (bt_{j-5}) della sequenza di corruzione (NV).

8. Dispositivo di protezione da attacchi informatici in una rete di comunicazione CAN, Controller Area Network, (20) di un veicolo comprendente un bus CAN (10) e una pluralità di nodi (11) associati a detto bus CAN (10) in rapporto di scambio di segnale e associati almeno in parte a unità di controllo di funzioni del veicolo, caratterizzato dal fatto di essere configurato per operare secondo il procedimento secondo una o più delle rivendicazioni da 1 a 7.

9. Dispositivo di protezione secondo la rivendicazione 8, caratterizzato dal fatto che comprende un modulo di firewall (261) configurato per eseguire almeno dette

operazioni di

analizzare il contenuto di messaggi CAN (M) e rendere non validi (F1, F2) messaggi non leciti (MF) rispetto a una verifica di integrità eseguita da un controllore CAN (13) di detti nodi (11),

e un modulo di memorizzazione per memorizzare detto insieme di regole (R) del firewall.

10. Dispositivo di protezione secondo la rivendicazione 8 o 9, caratterizzato dal fatto che

detto dispositivo di protezione (26) è disposto fra un controllore CAN (13) e un ricetrasmettitore CAN (12) di un nodo CAN.

11. Dispositivo di protezione secondo la rivendicazione 8 o 9, caratterizzato dal fatto che

detto dispositivo di protezione (26) è disposto interposto fra due reti CAN (20A, 20B) in associazione a un gateway (18).

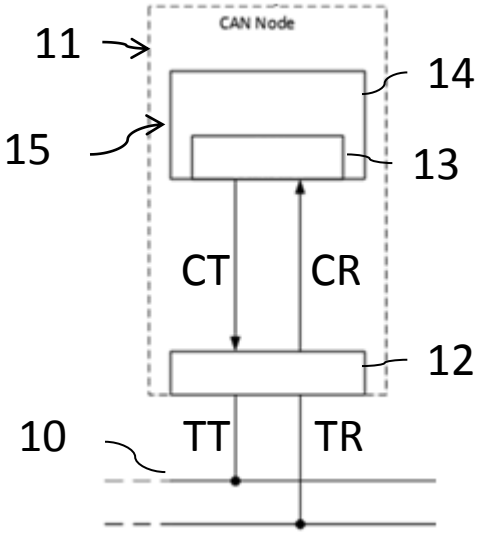
CAN Node
11
14
15
13
CT
CR
12
10
TT
TR

Fig. 1A

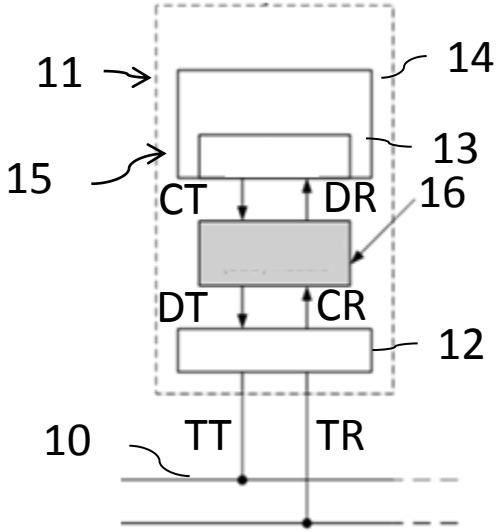
11
14
13
15
CT
DR
16
DT
CR
12
10
TT
TR

Fig. 1B

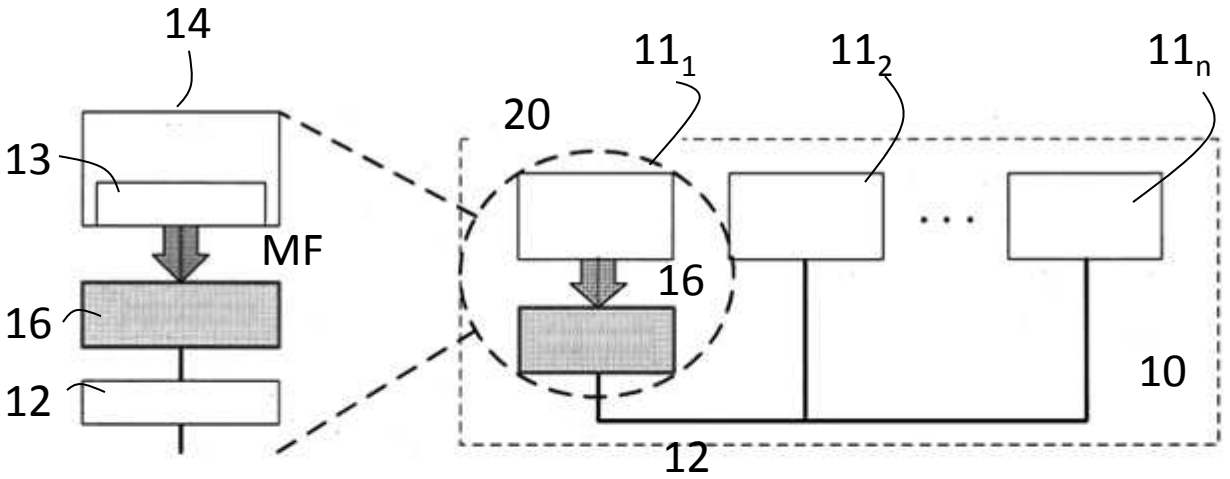
14
13
MF
16
12
20
11_1
11_2
11_n
16
10
12

Fig. 2

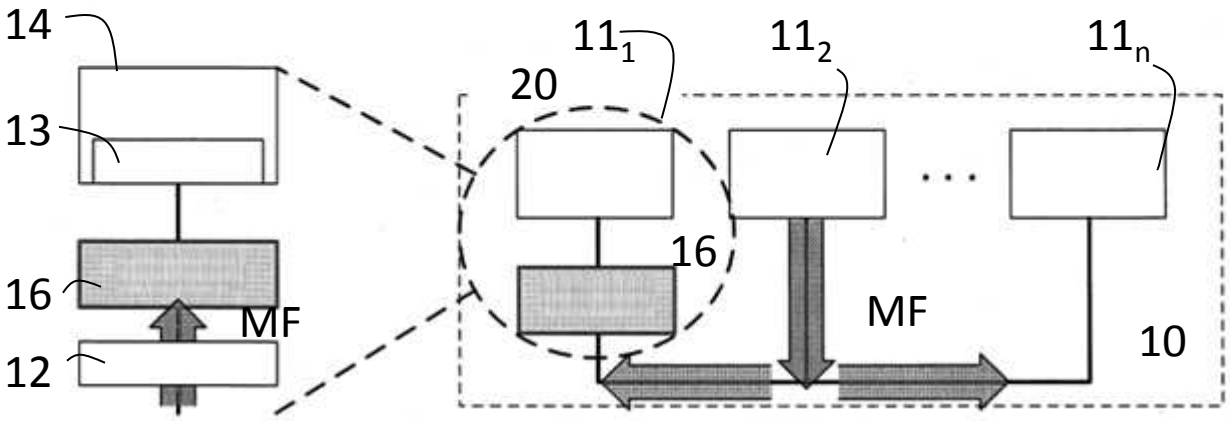
14
13
16
MF
12
20
11_1
11_2
11_n
16
MF
10

Fig. 3

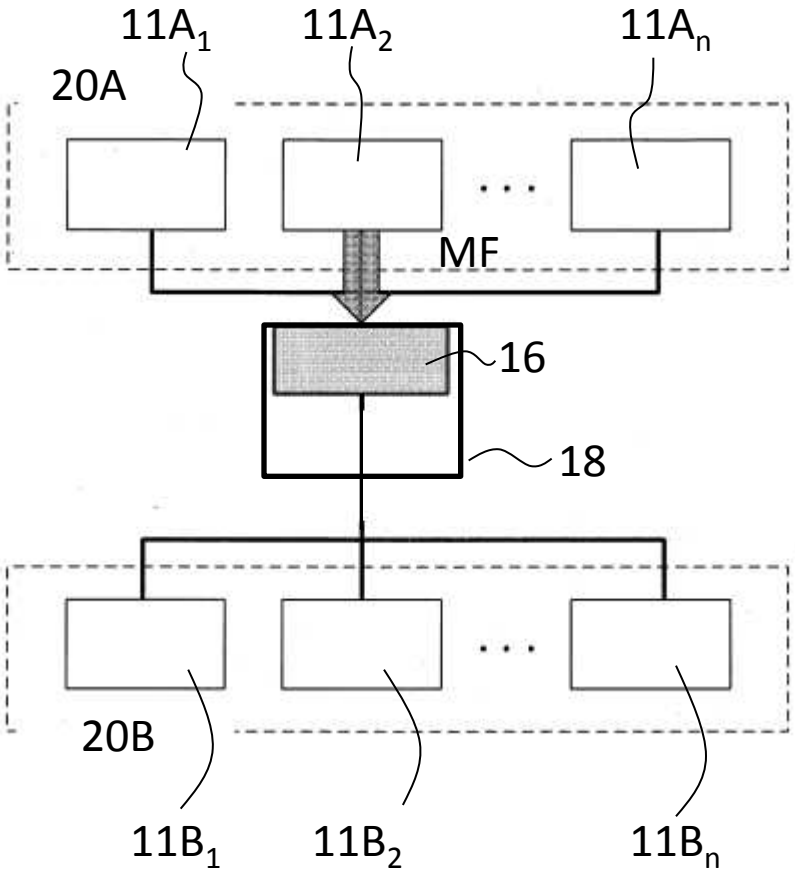

Fig. 4

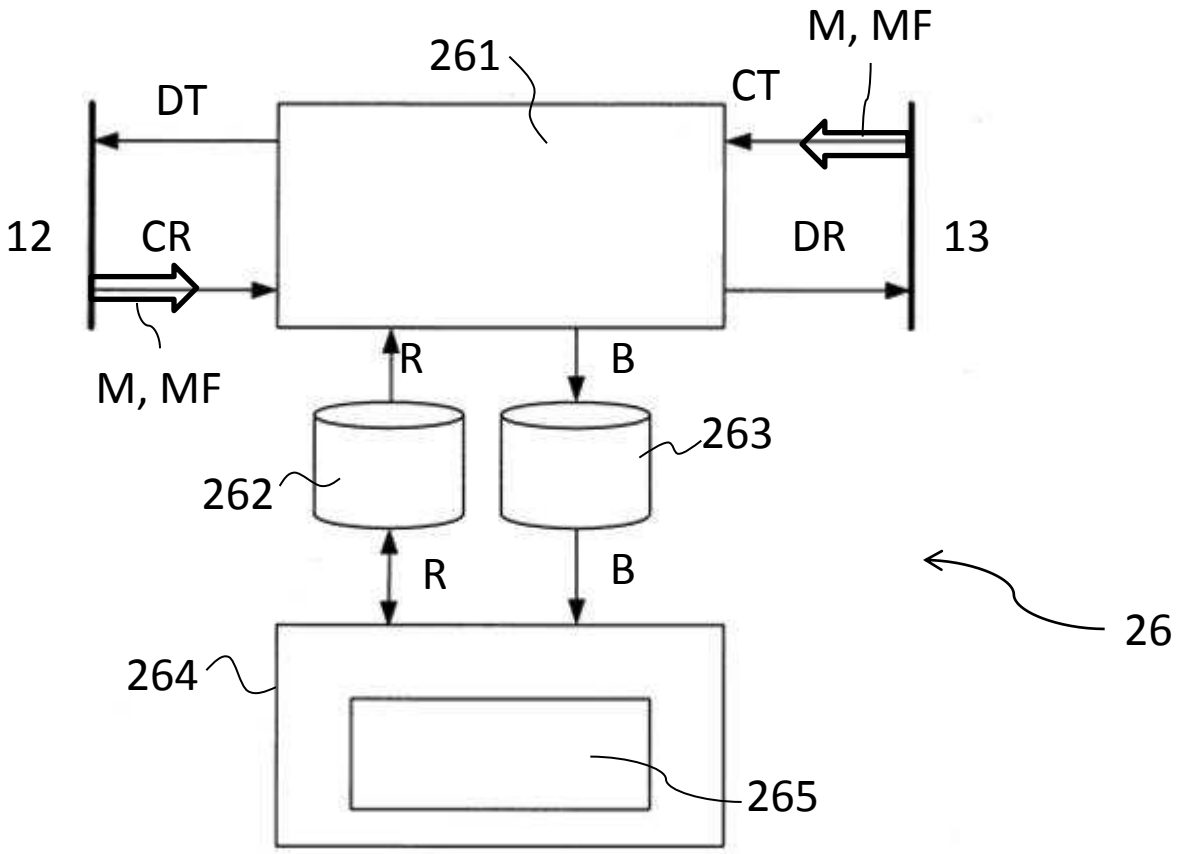

Fig. 5

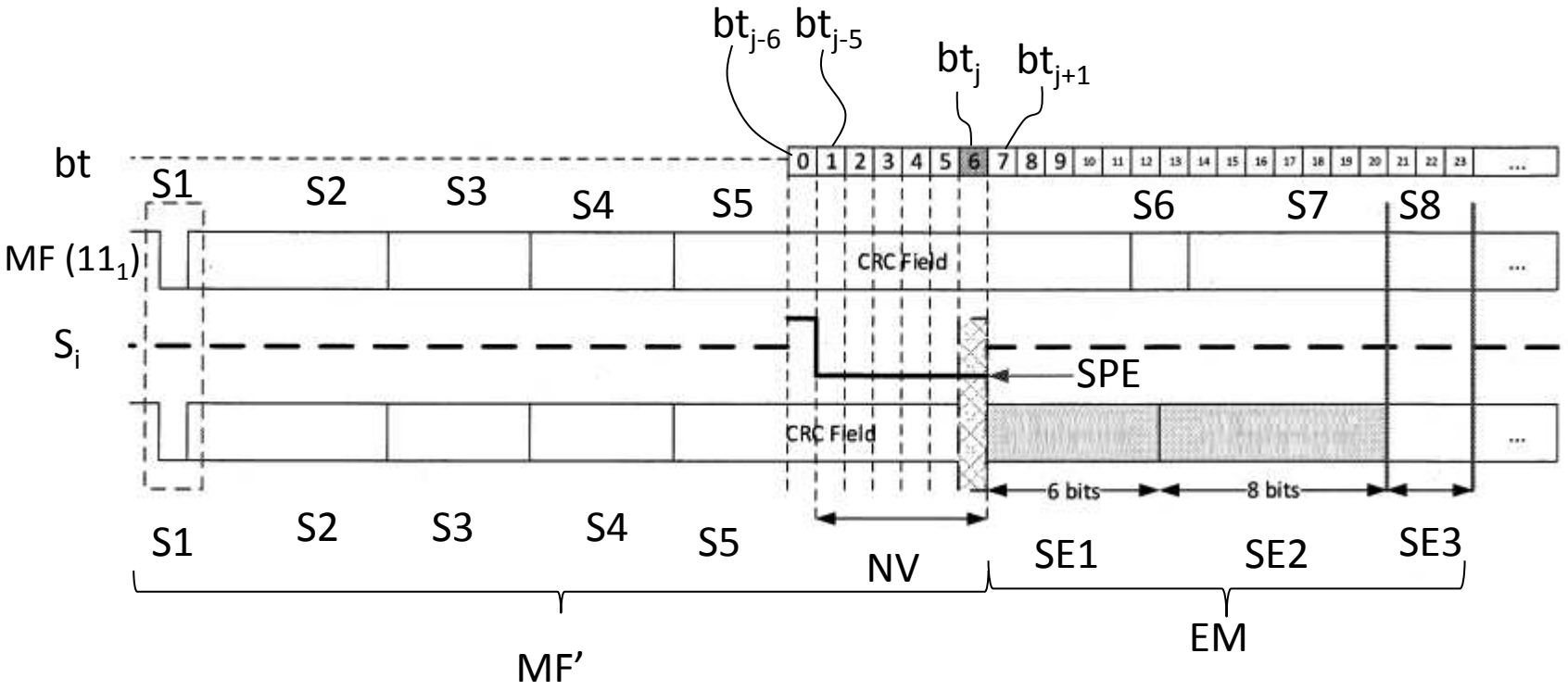
bt
MF (11₁)
Sᵢ
btj-6
btj-5
btj
btj+1
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 ...
S1
S2
S3
S4
S5
S6
S7
S8
CRC Field
SPE
6 bits
8 bits
NV
SE1
SE2
SE3
MF'
EM

Fig. 6

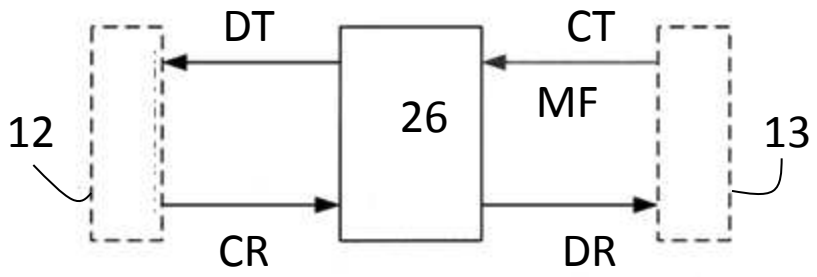

Fig. 7A

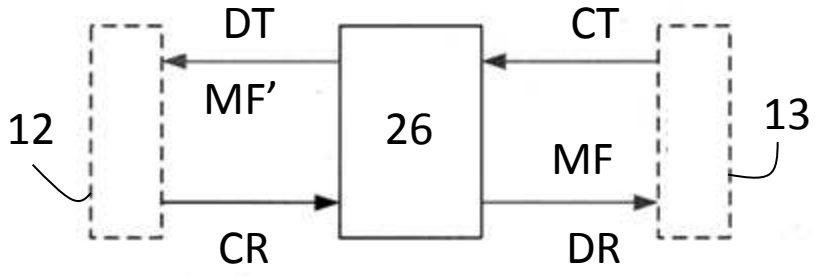

Fig. 7B

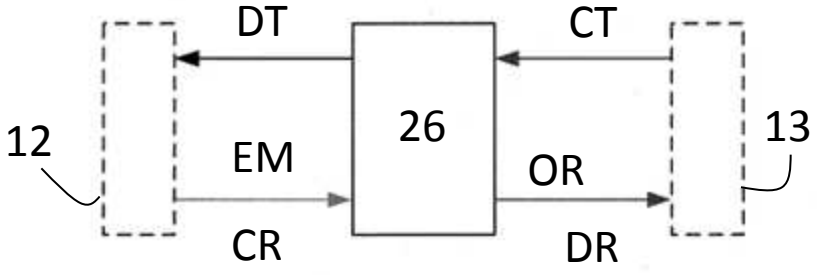

Fig. 7C

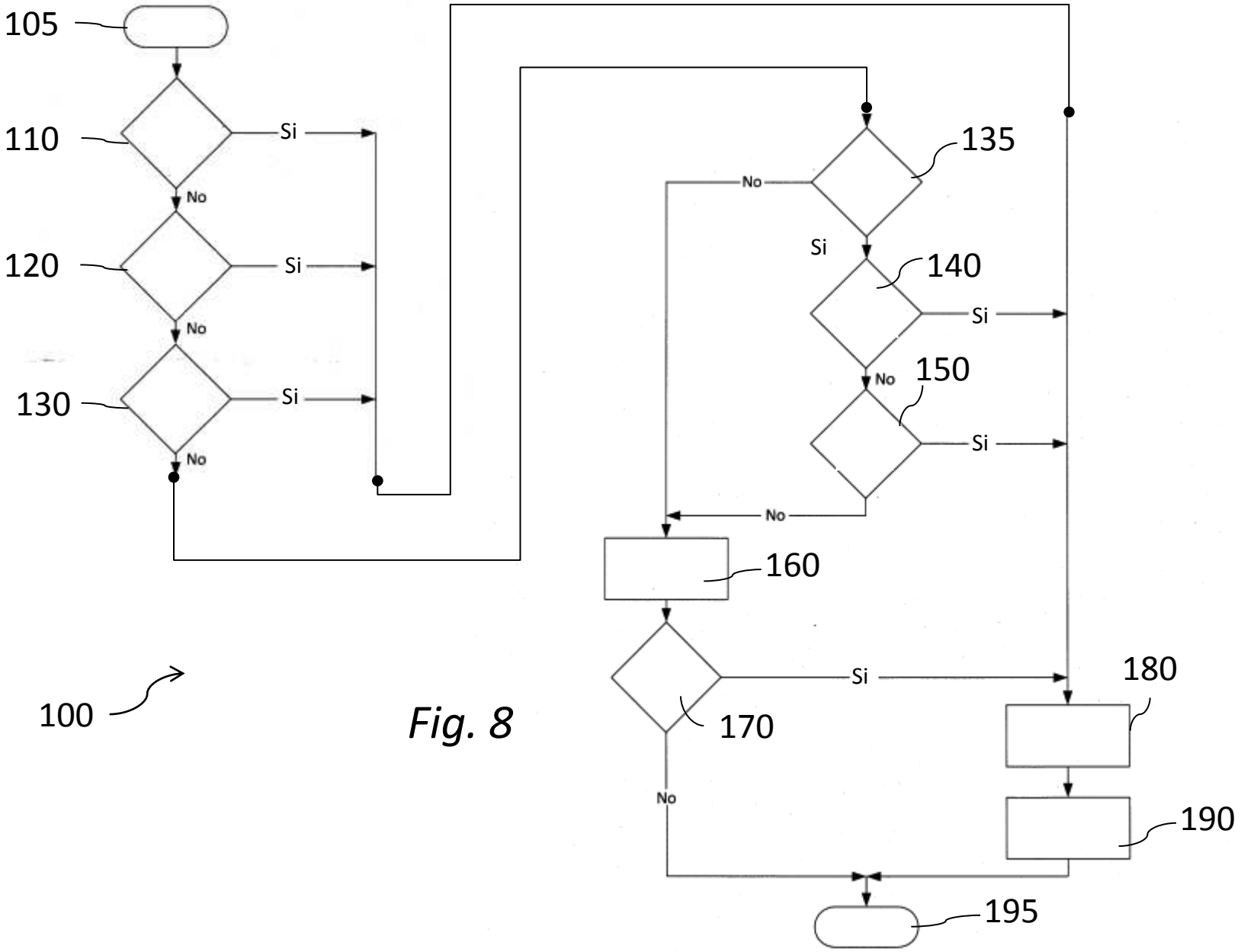
105
110
Si
No
120
Si
No
130
Si
No
135
No
Si
140
Si
No
150
Si
No
160
Si
170
No
180
190
195
100

Fig. 8

Ministero dello Sviluppo Economico

Direzione generale per la tutela della proprietà industriale

Ufficio Italiano Brevetti e Marchi

ATTESTATO DI BREVETTO PER INVENZIONE INDUSTRIALE

Il presente brevetto viene concesso per l'invenzione oggetto della domanda:

N. 102018000021550

TITOLARE/I:	• MAGNETI MARELLI S.P.A. 50.0% • UNIVERSITA' DI PISA 50.0%
	Crovini Giorgio
DOMICILIO:	Buzzi, Notaro & Antonielli d'Oulx S.r.l. Corso Vittorio Emanuele II, 6 10123 Torino
INVENTORE/I:	• ROSADINI Christian • NESCI Walter • BALDANZI Luca • CROCETTI Luca • FANUCCI Luca
TITOLO:	Procedimento di protezione da attacchi informatici al veicolo e corrispondente dispositivo
CLASSIFICA:	H04L
DATA DEPOSITO:	31/12/2018

Roma, 26/03/2021

Il Dirigente della Divisione VII
Loredana Guglielmetti

Via Molise 19 - 00187 Roma
tel. +39 06 4705 5800 - e-mail contactcenteruibm@mise.gov.it - www.mise.gov.it