

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7616901号
(P7616901)

(45)発行日 令和7年1月17日(2025.1.17)

(24)登録日 令和7年1月8日(2025.1.8)

(51)国際特許分類

FI

G 0 6 F 21/55 (2013.01)

G 0 5 B 9/02 (2006.01)

G 0 5 B 19/048 (2006.01)

G 0 6 F 21/55 3 2 0

G 0 5 B 9/02 A

G 0 5 B 19/048

請求項の数 4 (全14頁)

(21)出願番号	特願2021-25704(P2021-25704)	(73)特許権者	509186579
(22)出願日	令和3年2月19日(2021.2.19)		日立Astemo株式会社
(65)公開番号	特開2022-127512(P2022-127512 A)	(74)代理人	茨城県ひたちなか市高場2520番地 110002365
(43)公開日	令和4年8月31日(2022.8.31)		弁理士法人サンネクスト国際特許事務所
審査請求日	令和5年6月7日(2023.6.7)	(72)発明者	ポリッツ ギョーム
前置審査			東京都千代田区丸の内一丁目6番6号 株式会社日立製作所内
		(72)発明者	井手口 恒太
			東京都千代田区丸の内一丁目6番6号 株式会社日立製作所内
		審査官	吉田 歩

最終頁に続く

(54)【発明の名称】 電子制御システム

(57)【特許請求の範囲】

【請求項1】

装置の動作を記録したログを読み込み、情報セキュリティに関するイベントであるセキュリティイベントを検出するセキュリティイベント解析部と、

機能安全に関するイベントであるセーフティイベントに対する対処であるセーフティ機能を実行するために作成されたセーフティ機能実行部と、

前記セキュリティイベントに対する対処であるセキュリティ機能が実行可能なセキュリティ機能実行部と、

前記セキュリティイベントに対応する前記セーフティ機能および前記セキュリティ機能の少なくとも一方を示す対応情報が格納される記憶部と、

前記セキュリティイベント解析部が検出した前記セキュリティイベントに対応する機能を前記対応情報に基づき特定し、特定した機能を前記セーフティ機能実行部および前記セキュリティ機能実行部の少なくとも一方に実行させる決定部と、を備え、

前記対応情報において、少なくとも1つの前記セキュリティイベントに分類される前記イベントは、前記セーフティ機能と対応するように記録され、

前記決定部は、前記セキュリティイベント解析部が検出した前記セキュリティイベントに対応するセーフティ機能が前記対応情報として格納されているか否かを判断し、前記セーフティ機能が前記対応情報として格納されている場合、前記セーフティ機能実行部に前記セーフティ機能を実行させ、

前記決定部は、前記セキュリティイベント解析部が検出した前記セキュリティイベントに

対応するセーフティ機能が前記対応情報として格納されておらず、かつ前記セキュリティイベントに対応するセキュリティ機能が前記対応情報として格納されている場合、前記セキュリティ機能実行部に前記セキュリティ機能を実行させる、電子制御システム。

【請求項 2】

装置の動作を記録したログを読み込み、情報セキュリティに関するイベントであるセキュリティイベントを検出するセキュリティイベント解析部と、

機能安全に関するイベントであるセーフティイベントに対する対処であるセーフティ機能を実行するために作成されたセーフティ機能実行部と、

前記セキュリティイベントに対する対処であるセキュリティ機能が実行可能なセキュリティ機能実行部と、

前記セキュリティイベントに対応する前記セーフティ機能および前記セキュリティ機能の少なくとも一方を示す対応情報が格納される記憶部と、

前記セキュリティイベント解析部が検出した前記セキュリティイベントに対応する機能を前記対応情報に基づき特定し、特定した機能を前記セーフティ機能実行部および前記セキュリティ機能実行部の少なくとも一方に実行させる決定部と、を備え、

前記対応情報において、少なくとも1つの前記セキュリティイベントに分類される前記イベントは、前記セーフティ機能と対応するように記録され、

前記決定部は、前記セキュリティイベント解析部が検出した前記セキュリティイベントに対応するセーフティ機能が前記対応情報として格納されているか否かを判断し、前記セーフティ機能が前記対応情報として格納されている場合、前記セーフティ機能実行部に前記セーフティ機能を実行させ、

前記ログを読み込み、前記セーフティイベントを検出するセーフティイベント解析部をさらに備え、

前記対応情報には、前記セーフティイベントに対応する前記セーフティ機能がさらに格納され、

前記決定部はさらに、前記対応情報に基づき、前記セーフティイベント解析部が検出した前記セーフティイベントに対応する前記セキュリティ機能を特定し、特定した前記セキュリティ機能を前記セキュリティ機能実行部に実行させる、電子制御システム。

【請求項 3】

請求項 2 に記載の電子制御システムにおいて、

前記セキュリティイベント解析部は、前記セーフティイベント解析部が検出する前記セーフティイベント、および前記ログに基づき前記セキュリティイベントを検出する、電子制御システム。

【請求項 4】

請求項 1 または請求項 2 に記載の電子制御システムにおいて、

前記セーフティ機能実行部は、ISO26262 Part 3 section 7.4.2.3の規定に適合する、電子制御システム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、電子制御システムに関する。

【背景技術】

【0002】

車両には多数の電子制御装置が搭載され、相互に通信を行うことで高度な処理を実現している。装置に不具合が発生した場合への備えとして機能安全があり、機能安全を脅かすセーフティイベントへの対応について従来から広く研究開発が行われている。近年は電子制御装置が外部と通信することが一般的となり、通信を介した攻撃など情報セキュリティに関するセキュリティイベントへの対処も求められる。特許文献 1 には、外部装置との通信処理を行う通信インタフェース部、サービス不能攻撃の有無を判定し、サービス不能攻撃を検出した場合、前記通信インタフェース部に受信制限を実施させるとともに、セキュ

10

20

30

40

50

リティ処理部に受信制限を行っていることを示す遮断情報データの送信データへの添付を指示する判定部と、前記判定部からの指示に従い、送信時にセーフティ処理部からの送信データに対し、前記外部装置からの受信データ中に含まれこの外部装置に送り返す折り返しデータを前記遮断情報データへ付け替えるセキュリティ処理部と、を有するセキュリティ処理部、および、受信データに含まれる所定のデータを基に、該受信データの完全性をチェックするためのブラックチャネル診断を実施するブラックチャネル診断部と、前記外部装置への送信データに対し、前記折り返しデータを含む、ブラックチャネル診断のための所定のデータを添付し、前記セキュリティ処理部に渡すブラックチャネル送出部と、を有するセーフティ処理部、を備える制御装置が開示されている。

【先行技術文献】

【特許文献】

【0003】

【文献】特開2017-215788号公報

【発明の概要】

【発明が解決しようとする課題】

【0004】

特許文献1に記載されている発明では、セキュリティイベントへ対処する機能を全て開発する必要がある。

【課題を解決するための手段】

【0005】

本発明の第1の態様による電子制御システムは、装置の動作を記録したログを読み込み、情報セキュリティに関するイベントであるセキュリティイベントを検出するセキュリティイベント解析部と、機能安全に関するイベントであるセーフティイベントに対する対処であるセーフティ機能を実行するために作成されたセーフティ機能実行部と、前記セキュリティイベントに対する対処であるセキュリティ機能が実行可能なセキュリティ機能実行部と、前記セキュリティイベントに対応する前記セーフティ機能および前記セキュリティ機能の少なくとも一方を示す対応情報が格納される記憶部と、前記セキュリティイベント解析部が検出した前記セキュリティイベントに対応する機能を前記対応情報に基づき特定し、特定した機能を前記セーフティ機能実行部および前記セキュリティ機能実行部の少なくとも一方に実行させる決定部と、を備え、前記対応情報において、少なくとも1つの前記セキュリティイベントに分類される前記イベントは、前記セーフティ機能と対応するように記録され、前記決定部は、前記セキュリティイベント解析部が検出した前記セキュリティイベントに対応するセーフティ機能が前記対応情報として格納されているか否かを判断し、前記セーフティ機能が前記対応情報として格納されている場合、前記セーフティ機能実行部に前記セーフティ機能を実行させ、前記決定部は、前記セキュリティイベント解析部が検出した前記セキュリティイベントに対応するセーフティ機能が前記対応情報として格納されておらず、かつ前記セキュリティイベントに対応するセキュリティ機能が前記対応情報として格納されている場合、前記セキュリティ機能実行部に前記セキュリティ機能を実行させる、電子制御システム。

本発明の第2の態様による電子制御システムは、装置の動作を記録したログを読み込み、情報セキュリティに関するイベントであるセキュリティイベントを検出するセキュリティイベント解析部と、機能安全に関するイベントであるセーフティイベントに対する対処であるセーフティ機能を実行するために作成されたセーフティ機能実行部と、前記セキュリティイベントに対する対処であるセキュリティ機能が実行可能なセキュリティ機能実行部と、前記セキュリティイベントに対応する前記セーフティ機能および前記セキュリティ機能の少なくとも一方を示す対応情報が格納される記憶部と、前記セキュリティイベント解析部が検出した前記セキュリティイベントに対応する機能を前記対応情報に基づき特定し、特定した機能を前記セーフティ機能実行部および前記セキュリティ機能実行部の少なくとも一方に実行させる決定部と、を備え、前記対応情報において、少なくとも1つの前記セキュリティイベントに分類される前記イベントは、前記セーフティ機能と対応するよ

10

20

30

40

50

うに記録され、前記決定部は、前記セキュリティイベント解析部が検出した前記セキュリティイベントに対応するセーフティ機能が前記対応情報として格納されているか否かを判断し、前記セーフティ機能が前記対応情報として格納されている場合、前記セーフティ機能実行部に前記セーフティ機能を実行させ、前記ログを読み込み、前記セキュリティイベントを検出するセーフティイベント解析部をさらに備え、前記対応情報には、前記セキュリティイベントに対応する前記セーフティ機能がさらに格納され、前記決定部はさらに、前記対応情報に基づき、前記セキュリティイベント解析部が検出した前記セキュリティイベントに対応する前記セキュリティ機能を特定し、特定した前記セキュリティ機能を前記セキュリティ機能実行部に実行させる、電子制御システム。

【発明の効果】

【0006】

本発明によれば、セキュリティイベントへの対処にセーフティイベントへの対応機能を用いることで、セキュリティイベントへ対処する機能の開発を低減できる。

【図面の簡単な説明】

【0007】

【図1】実施の形態における電子制御システムの構成図

【図2】機能安全対処表の一例を示す図

【図3】情報安全対処表の一例を示す図

【図4】ゲートウェイの処理を示すフローチャート

【図5】変形例1におけるゲートウェイの処理を示すフローチャート

【図6】変形例7におけるゲートウェイの構成図

【発明を実施するための形態】

【0008】

（用語の定義）

本明細書では「セーフティ」および「セキュリティ」は次の意味で用いる。「セーフティ」とは、機能安全を意味し、たとえばISO 26262に定義されている「電気電子システムの機能不全のふるまいにより引き起こされるハザードが原因となる、不合理なリスクの不在」である。「セキュリティ」とは、情報セキュリティを意味し、たとえば情報の機密性、完全性、可用性が保たれることとである。なお以下では「セキュリティ」を「情報安全」とも呼ぶ。

【0009】

また本明細書では、セーフティが脅かされている状態、またはセーフティが保たれていない状態を「セーフティ事例」や「セーフティイベント」と呼び、セーフティ事例を解消または緩和するための動作や処理を「セーフティ機能」と呼ぶ。同様に、セキュリティが脅かされている状態、またはセキュリティが保たれていない状態を「セキュリティ事例」や「セキュリティイベント」と呼び、セキュリティ事例を解消または緩和するための動作や処理を「セキュリティ機能」と呼ぶ。

【0010】

セーフティ事例にはたとえば、装置の故障や通信の断絶などが含まれる。セキュリティ事例にはたとえば、パラメータの書き換え、侵入の検知、および通信品質の低下などが含まれる。セーフティ機能には、機能を低下させて動作を維持する縮退動作の有効化が含まれる。セキュリティ機能には、パラメータの初期化などが含まれる。

【0011】

—実施の形態—

以下、図1～図4を参照して、電子制御システム1の実施の形態を説明する。

【0012】

図1は、実施の形態における電子制御システム1の構成図である。電子制御システム1は、車両に搭載されるゲートウェイ20と、ECU30と、TCU40とを含む。ゲートウェイ20とTCU40との間の通信、およびゲートウェイ20とECU30との間の通信に用いる通信規格は任意であり、たとえばIEEE 802.3が用いられる。

10

20

30

40

50

【0013】

ゲートウェイ20は、車両の内部における通信を統括する装置である。ECU30は、電子制御装置（Electronic Control Unit）であり、車両に搭載されるさまざまな機器からログを収集してゲートウェイ20に提供する。さらにECU30は、ゲートウェイ20の動作指令に基づきセーフティ対応およびセキュリティ対応を行う。TCU40は、テレマティクス制御ユニット（Telematic control unit）であり、車両の外部と無線通信を行う。TCU40が外部から受信したデータは、ゲートウェイ20を介してECU30に送信される。

【0014】

ゲートウェイ20およびECU30は、中央演算装置であるCPU、読み出し専用の記憶装置であるROM、および読み書き可能な記憶装置であるRAMを備え、CPUがROMに格納されるプログラムをRAMに展開して実行することで後述する機能を実現する。ゲートウェイ20およびECU30は、CPU、ROM、およびRAMの組み合わせの代わりに書き換え可能な論理回路であるFPGA（Field Programmable Gate Array）や特定用途向け集積回路であるASIC（Application Specific Integrated Circuit）により実現されてもよい。またゲートウェイ20およびECU30は、CPU、ROM、およびRAMの組み合わせの代わりに、異なる構成の組み合わせ、たとえばCPU、ROM、RAMとFPGAの組み合わせにより実現されてもよい。

【0015】

ゲートウェイ20はその機能として、ログ収集部21と、機能安全解析部221と、情報安全解析部222と、GW記憶部23と、決定部24と、通信部29とを備える。ログ収集部21、機能安全解析部221、情報安全解析部222、決定部24、および通信部29は、前述のCPUなどにより実現される。GW記憶部23は、不揮発性の記憶装置、たとえばフラッシュメモリにより実現される。なお以下では、機能安全解析部221を「セーフティイベント解析部」とも呼び、情報安全解析部222を「セキュリティイベント解析部」とも呼ぶ。

【0016】

ログ収集部21は、ECU30のECU記憶部33からセーフティログ331およびセキュリティログ332を収集してGW記憶部23に格納する。ただし図1では作図の都合によりGW記憶部23にはセーフティログ331およびセキュリティログ332を記載していない。機能安全解析部221は、GW記憶部23に格納されたセーフティログ331を解析してセーフティ事例を特定し、イベントIDを付与する。本実施の形態では、セーフティ事例のイベントIDは「P」と数字の組み合わせにより表現する。機能安全解析部221はたとえば、ログに含まれる文字列とあらかじめ定められた文字列との一致、またはログに含まれる数値と所定の閾値との大小関係により、セーフティ事例を特定する。

【0017】

情報安全解析部222は、GW記憶部23に格納されたセキュリティログ332を解析してセキュリティ事例を特定し、イベントIDを付与する。本実施の形態では、セキュリティ事例のイベントIDは「Q」と数字の組み合わせにより表現する。情報安全解析部222はたとえば、ログに含まれる文字列とあらかじめ定められた文字列との一致、またはログに含まれる数値と所定の閾値との大小関係により、セキュリティ事例を特定する。

【0018】

GW記憶部23には、あらかじめ作成された、機能安全対処表231および情報安全対処表232が格納される。機能安全対処表231は、セキュリティ事例への対処方法が記載されている。情報安全対処表232には、セーフティ事例への対処方法が記載されている。機能安全対処表231および情報安全対処表232の詳細は後述する。決定部24は、機能安全解析部221および情報安全解析部222が検出したセキュリティ事例およびセーフティ事例に対する対処を決定し、その決定内容をECU30に送信する。決定部24は、それぞれの事例に対する対処を決定するために、機能安全対処表231および情報安全対処表232を参照する。なお以下では、機能安全対処表231および情報安全対処

10

20

30

40

50

表 2 3 2 をあわせて、対処表 2 3 3 とも呼ぶ。

【 0 0 1 9 】

通信部 2 9 は、ゲートウェイ 2 0 の本来的な機能を実現し、たとえば T C U 4 0 から受信したデータの宛先決定やフィルタリングなどを行う。ただし通信部 2 9 が行う処理の詳細は本実施の形態では説明しない。

【 0 0 2 0 】

E C U 3 0 は、その機能として、機能安全機能実行部 3 1 と、情報安全機能実行部 3 2 と、E C U 記憶部 3 3 と、車両内ログ収集部 3 4 とを備える。機能安全機能実行部 3 1 および情報安全機能実行部 3 2 は、前述の C P U などにより実現される。機能安全機能実行部 3 1 および情報安全機能実行部 3 2 は、G W 2 0 の決定部 2 4 が送信する動作指令に基づき動作する。決定部 2 4 が送信する動作指令は、あらかじめ定められたいずれかの動作指令あり、本実施の形態ではこれらの指令をアルファベットと数字を組み合わせた識別子で表す。さらにこの識別子のアルファベットは、機能安全機能実行部 3 1 を動作させる識別子には「E」を用い、情報安全機能実行部 3 2 を動作させる識別子には「F」を用いる。

【 0 0 2 1 】

機能安全機能実行部 3 1 は、ゲートウェイ 2 0 から送信される動作指令に基づき、セーフティ事例への対処を行う。機能安全機能実行部 3 1 はたとえば、ゲートウェイ 2 0 からの動作指令に基づき、車両の動力源、たとえばモータに対して停止指令を出力する。機能安全機能実行部 3 1 の動作は、国際規格である「ISO26262 Part 3 section 7.4.2.3」の規定に適合するものである。情報安全機能実行部 3 2 は、ゲートウェイ 2 0 から送信される動作指令に基づき、セキュリティ事例への対処を行う。情報安全機能実行部 3 2 はたとえば、ゲートウェイ 2 0 からの動作指令に基づき、前照灯のコントローラに対してパラメータの初期値指令を出力する。なお以下では、機能安全機能実行部 3 1 を「セーフティ機能実行部」とも呼び、情報安全機能実行部 3 2 を「セキュリティ機能実行部」とも呼ぶ。

【 0 0 2 2 】

車両内ログ収集部 3 4 は、車両に搭載されるさまざまな装置から動作ログを収集し、E C U 記憶部 3 3 にセーフティログ 3 3 1 およびセキュリティログ 3 3 2 として格納する。セーフティログ 3 3 1 およびセキュリティログ 3 3 2 は、ログの収集先の装置により分類されてもよいし、ログの内容に基づき分類されてもよい。具体的には以下のとおりである。たとえば車両の移動に関与する、モータやブレーキを制御する装置のログはセーフティログ 3 3 1 として格納し、それ以外の前照灯を制御する装置のログはセキュリティログ 3 3 2 として格納してもよい。またたとえば、ログがあらかじめ「debug」、「notice」、「warn」、「error」と深刻さに応じてタグ付けされている場合には、「debug」と「notice」のタグが付されたログはセキュリティログ 3 3 2 として格納し、「warn」と「error」のタグが付されたログはセーフティログ 3 3 1 として格納する。

【 0 0 2 3 】

E C U 記憶部 3 3 は、不揮発性の記憶装置、たとえばフラッシュメモリにより実現される。E C U 記憶部 3 3 には、セーフティログ 3 3 1 およびセキュリティログ 3 3 2 が格納される。

【 0 0 2 4 】

図 2 は、機能安全対処表 2 3 1 の一例を示す図である。機能安全対処表 2 3 1 は複数のレコードを含む。機能安全対処表 2 3 1 の各レコードは、イベント I D 2 3 1 1、対象 2 3 1 2、種別 2 3 1 3、および対処 2 3 1 4 のフィールドを有する。イベント I D 2 3 1 1 のフィールドには、イベントの識別子が格納される。対象 2 3 1 2 のフィールドには、対処を行う装置の識別情報が格納される。種別 2 3 1 3 のフィールドには、対処の種類を示す情報が格納されるが、機能安全対処表 2 3 1 では「セーフティ」のみが格納される。対処 2 3 1 4 のフィールドには、対処として実行する処理の内容、または対処として実行する処理の識別子が格納される。

【 0 0 2 5 】

図 2 に示す最初のレコードは、イベント P 1 が発生した際には E C U 3 0 においてセー

10

20

30

40

50

フティに分類される「E 1」の処理を実行することが記載されている。また図 2 に示す 3 番目のレコードは、イベント P 3 が発生した際にはゲートウェイ 2 0 においてセーフティに分類される「E 3」の処理を実行することが記載されている。

【0026】

図 3 は、情報安全対処表 2 3 2 の一例を示す図である。情報安全対処表 2 3 2 は複数のレコードを含む。情報安全対処表 2 3 2 の各レコードは、イベント ID 2 3 2 1、対象 2 3 2 2、種別 2 3 2 3、および対処 2 3 2 4 のフィールドを有する。各フィールドに格納される情報は、機能安全対処表 2 3 1 の同名のフィールドに格納される情報と同様なので詳細は省略する。ただし種別 2 3 2 3 のフィールドには、「セーフティ」だけでなく「セキュリティ」も格納されうる。

10

【0027】

図 3 に示す最初のレコードは、イベント Q 1 が発生した際には ECU 3 0 において「セキュリティ」に分類される「F 1」の処理を実行することが記載されている。図 3 に示す 2 番目のレコードは、イベント Q 2 が発生した際には ECU 3 0 において「セーフティ」に分類される「E 5」の処理を実行することが記載されている。図 3 に示す 3 番目のレコードは、イベント Q 3 が発生した際には ECU 3 0 において「セーフティ」に分類される「E 2」の処理、および「セキュリティ」に分類される「F 2」の処理を実行することが記載されている。

【0028】

図 4 は、ゲートウェイ 2 0 の処理を示すフローチャートである。ゲートウェイ 2 0 のログ収集部 2 1、機能安全解析部 2 2 1、情報安全解析部 2 2 2、および決定部 2 4 は、ゲートウェイ 2 0 の電源がオンの間は図 4 に示す処理を繰り返し実行する。ステップ S 3 0 1 では、ログ収集部 2 1 が ECU 3 0 からログ、すなわちセキュリティログ 1 2 1 およびセーフティログ 1 2 2 を収集する。ゲートウェイ 2 0 は、ステップ S 3 0 1 の処理が完了すると、ステップ S 3 0 2 の処理とステップ S 3 0 5 の処理を並列に実行する。

20

【0029】

ステップ S 3 0 2 では機能安全解析部 2 2 1 は、ステップ S 3 0 1 において収集されたセーフティログ 3 3 1 を解析してセーフティ事例を特定し、イベント ID を付与する。続くステップ S 3 0 3 では決定部 2 4 は、機能安全対処表 2 3 1 を参照し、セーフティ機能を有効化すべきセーフティ状態にあるか否かを判断する。決定部 2 4 は、セーフティ機能を有効化すべきと判断する場合はステップ S 3 0 4 に進み、セーフティ機能を有効化すべきではないと判断する場合はステップ S 3 0 1 に戻る。本ステップの具体的な処理は次のとおりである。

30

【0030】

決定部 2 4 は、ステップ S 3 0 2 において特定されたイベント ID が機能安全対処表 2 3 1 のイベント ID 2 3 1 1 の欄に含まれるレコードを検索する。決定部 2 4 は、そのイベント ID をイベント ID 2 3 1 1 の欄に含むレコードが見つかった場合にはステップ S 3 0 3 を肯定判断し、該当するレコードが見つからない場合にはステップ S 3 0 3 を否定判断する。また決定部 2 4 は、ステップ S 3 0 2 においてイベント ID が特定されなかった場合もステップ S 3 0 3 において否定判断する。

40

【0031】

ステップ S 3 0 4 では決定部 2 4 は、機能安全対処表 2 3 1 または情報安全対処表 2 3 2 を参照してイベント ID に対応する対処を特定し、特定した対処を実行させる。対処を実行させる対象は、ECU 3 0 またはゲートウェイ 2 0 の通信部 2 9 である。

【0032】

ステップ S 3 0 5 では情報安全解析部 2 2 2 は、ステップ S 3 0 1 において収集されたセキュリティログ 3 3 2 を解析してセキュリティ事例を特定し、イベント ID を付与する。続くステップ S 3 0 6 では決定部 2 4 は、情報安全対処表 2 3 2 を参照し、セーフティ機能を有効化すべきセキュリティ状態にあるか否かを判断する。決定部 2 4 は、セーフティ機能を有効化すべきセキュリティ状態にあると判断する場合はステップ S 3 0 4 に進み

50

、セーフティ機能を有効化すべきセキュリティ状態にないと判断する場合はステップ S 3 0 7 に戻る。本ステップの具体的な処理は次のとおりである。

【 0 0 3 3 】

決定部 2 4 は、ステップ S 3 0 5 において特定されたイベント ID が情報安全対処表 2 3 2 のイベント ID 2 3 2 1 の欄に含まれるレコードを検索する。決定部 2 4 は、そのイベント ID をイベント ID 2 3 2 1 の欄に含むレコードを特定し、そのレコードの種別 2 3 2 3 が「セーフティ」の場合は肯定判断する。決定部 2 4 は、そのイベント ID をイベント ID 2 3 2 1 の欄に含むレコードが発見できない場合や、そのレコードの種別 2 3 2 3 が「セキュリティ」の場合は否定判断する。

【 0 0 3 4 】

ステップ S 3 0 7 では決定部 2 4 は、情報安全対処表 2 3 2 を参照し、セキュリティ機能を有効化すべきセキュリティ状態にあるか否かを判断する。決定部 2 4 は、セキュリティ機能を有効化すべきセキュリティ状態にあると判断する場合はステップ S 3 0 8 に進み、セキュリティ機能を有効化すべきセキュリティ状態にないと判断する場合はステップ S 3 0 1 に戻る。本ステップの具体的な処理は次のとおりである。

【 0 0 3 5 】

決定部 2 4 は、ステップ S 3 0 5 において特定されたイベント ID が情報安全対処表 2 3 2 のイベント ID 2 3 2 1 の欄に含まれるレコードを検索する。決定部 2 4 は、そのイベント ID をイベント ID 2 3 2 1 の欄に含むレコードを特定し、そのレコードの種別 2 3 2 3 が「セキュリティ」の場合は肯定判断する。決定部 2 4 は、そのイベント ID をイベント ID 2 3 2 1 の欄に含むレコードが発見できない場合は否定判断する。以上が図 3 に示す処理の説明である。

【 0 0 3 6 】

上述した実施の形態によれば、次の作用効果が得られる。

(1) 電子制御システム 1 は、車両に搭載される様々な装置の動作を記録したログを読み込み、情報セキュリティに関するイベントであるセキュリティイベントを検出するセキュリティイベント解析部 2 2 2 と、機能安全に関するイベントであるセーフティイベントに対する対処であるセーフティ機能を実行するために作成されたセーフティ機能実行部 3 1 と、セキュリティイベントに対する対処であるセキュリティ機能が実行可能なセキュリティ機能実行部 3 2 と、セキュリティイベントに対応するセーフティ機能およびセキュリティ機能の少なくとも一方を示す対処表 2 3 3 が格納される G W 記憶部 2 3 と、セキュリティイベント解析部 2 2 2 が検出したセキュリティイベントに対応する機能に対応情報に基づき特定し、特定した機能をセーフティ機能実行部 3 1 およびセキュリティ機能実行部 3 2 の少なくとも一方に実行させる決定部 2 4 と、を備える。対処表 2 3 3 において、図 3 に示す例におけるイベント Q 2 や Q 3 のように、少なくとも 1 つのセキュリティイベントに分類されるイベントは、セーフティ機能と対応するように記録される。

【 0 0 3 7 】

そのため、セーフティ機能実行部 3 1 を利用して一部のセキュリティイベントに対応できるため、セキュリティ機能実行部 3 2 はその一部を除いたセキュリティイベントに対応すればよく、セキュリティ機能実行部 3 2 の開発を低減できる。具体的には、セキュリティ機能実行部 3 2 が実行する機能を減らすことができるので、開発工数および検証工数を削減でき、コストも削減される。

【 0 0 3 8 】

本実施の形態における技術的思想は次のとおりである。セーフティへの対応は、ISO 26 262 などのように規格化されており、長年の研究開発に基づき熟練されている。その一方で、セキュリティへの対応は、セーフティに比較すれば歴史が浅く、新たに対処すべき事項が発見されることも多い。直接的な解決手法として、セーフティ事案とセキュリティ事案のそれぞれに対して個別の対応をとることができるが、同一または包含関係にある対応策も存在する。換言すると、一部のセキュリティ事案はあるセーフティ対応策により対応が可能であり、一部のセーフティ事案はあるセキュリティ対応策により対応が可能である。

10

20

30

40

50

【0039】

ここで、セキュリティ対応とセーフティ対応の開発の歴史、や資産の活用を考慮すると、開発済みのセーフティ対応策は開発済のセキュリティ対応策よりも多く、安定性の面でも利点があると考えられる。そのため、セーフティ対応策により対処可能なセキュリティ事案を事前に特定しておき、情報安全対処表232に記載しておくことでそのようなセキュリティ事例はセーフティ対応策により対応する。これによりセキュリティ対応策の開発を低減でき、コスト低減および開発期間短縮の利点が得られる。

【0040】

(2) 電子制御システム1は、ログを読み込み、セーフティイベントを検出するセーフティイベント解析部221を備える。対処表233には、セーフティイベントに対応するセーフティ機能が示された機能安全対処表231が含まれる。決定部24は、対処表233に基づき、セーフティイベント解析部22が検出したセーフティイベントに対応するセキュリティ機能を特定し、特定したセキュリティ機能をセキュリティ機能実行部32に実行させる。そのため電子制御システム1は、セーフティイベントに対する対処も実行できる。

10

【0041】

(3) セーフティ機能実行部31は、ISO26262 Part 3 section 7.4.2.3の規定に適合する。そのため電子制御システム1は、信頼性の高いセーフティ機能実行部31を用いてセキュリティイベントに対処できる。

【0042】

(変形例1)

20

上述した実施の形態における処理を簡略化してもよい。たとえば、並列処理を特に行うことなく、有効化すべき各機能を特定して実行してもよい。

【0043】

図5は、変形例1におけるゲートウェイ20の処理を示すフローチャートである。図4と同一の処理には同一のステップ番号を付して説明を省略する。ステップS301では、ログ収集部21がECU30からログ、すなわちセキュリティログ121およびセーフティログ122を収集する。続くステップS302Aでは、機能安全解析部221は、ステップS301において収集されたセーフティログ331を解析してセーフティ事例を特定し、イベントIDを付与する。続くステップS305Aでは、情報安全解析部222は、ステップS301において収集されたセキュリティログ332を解析してセキュリティ事例を特定し、イベントIDを付与する。

30

【0044】

続くステップS311では決定部24は、機能安全対処表231および情報安全対処表232を参照し、ステップS302AおよびS305Aにおいて特定されたイベントIDBに対応する対処を特定する。たとえば図2や図3の例によれば、対処として「E2」や「F1」などが特定される。

【0045】

続くステップS312では決定部24は、有効化すべきセーフティ機能が存在するか否かを判断する。決定部24は、ステップS312において肯定判断する場合はステップS304Aに進み、否定判断する場合はステップS313に進む。たとえば決定部24は、ステップS311において特定された対処において、「E」を含む識別子が存在する場合には、有効化すべきセーフティ機能が存在すると判断する。ただし決定部24は、ステップS302AおよびS305Aにおいて特定されたレコードの種別2313または種別2323の欄の値が「セーフティ」である場合にステップS312を肯定判断してもよい。

40

【0046】

ステップS304Aでは決定部24は、ステップS311において有効化すべきと判断したセーフティ機能を有効化してステップS312に進む。具体的には決定部24は、有効化すべきセーフティ機能の識別子、たとえば「E1」などを、その機能を実行する装置、たとえばECU30に送信する。

【0047】

50

ステップ S 3 1 3 では決定部 2 4 は、有効化すべきセキュリティ機能が存在するか否かを判断する。決定部 2 4 は、ステップ S 3 1 3 において肯定判断する場合はステップ S 3 0 8 A に進み、否定判断する場合はステップ S 3 0 1 に戻る。たとえば決定部 2 4 は、ステップ S 3 1 1 において特定された対処において、「F」を含む識別子が存在する場合には、有効化すべきセキュリティ機能が存在すると判断する。ただし決定部 2 4 は、ステップ S 3 0 2 A および S 3 0 5 A において特定されたレコードの種別 2 3 1 3 または種別 2 3 2 3 の欄の値が「セキュリティ」である場合にステップ S 3 1 3 を肯定判断してもよい。

【0048】

ステップ S 3 0 8 A では決定部 2 4 は、ステップ S 3 1 1 において有効化すべきと判断したセキュリティ機能を有効化してステップ S 3 0 1 に戻る。具体的には決定部 2 4 は、有効化すべきセキュリティ機能の識別子、たとえば「F 1」などを、その機能を実行する装置、たとえば E C U 3 0 に送信する。以上が図 5 の説明である。

【0049】

この変形例 1 によれば、より簡素な処理により上述した実施の形態と同様の作用効果を得ることができる。また本変形例では機能安全対処表 2 3 1 と情報安全対処表 2 3 2 とを一体化して G W 記憶部 2 3 に格納してもよい。

【0050】

(変形例 2)

上述した実施の形態では、ゲートウェイ 2 0 には通信部 2 9 に加えて、ログ収集部 2 1、機能安全解析部 2 2 1、情報安全解析部 2 2 2、G W 記憶部 2 3、および決定部 2 4 が含まれた。しかし、ログ収集部 2 1、機能安全解析部 2 2 1、情報安全解析部 2 2 2、G W 記憶部 2 3、および決定部 2 4 の機能がそれぞれ異なる装置に搭載されてもよい。図 4 のフローチャートで示したように、ログ収集部 2 1、機能安全解析部 2 2 1、情報安全解析部 2 2 2、および決定部 2 4 の処理は相互に関係するが、それぞれが異なる装置により実現される機能であっても、通信により情報を授受することで動作に支障がない。

【0051】

(変形例 3)

上述した実施の形態において、電子制御システム 1 は、機能安全解析部 2 2 1 を備えなくてもよい。この場合には図 4 に示したステップ S 3 0 2 およびステップ S 3 0 3 の処理が実行されない。

【0052】

(変形例 4)

上述した実施の形態において、情報安全解析部 2 2 2 は、機能安全解析部 2 2 1 による解析結果を参照してもよい。この場合は、セーフティイベントと関連のあるセキュリティイベントの検出に有用である。すなわち本変形例ではセキュリティイベント解析部 2 2 2 は、セーフティイベント解析部 2 2 1 が検出するセーフティイベント、およびセキュリティログ 3 3 2 に基づきセキュリティイベントを検出する。

【0053】

(変形例 5)

機能安全機能実行部 3 1 と情報安全機能実行部 3 2 は、それぞれ別の装置に搭載されてもよい。さらに機能安全機能実行部 3 1 と情報安全機能実行部 3 2 のそれぞれが、複数の装置に搭載されてもよい。この場合には、機能安全対処表 2 3 1 の対象 2 3 1 2 および情報安全対処表 2 3 2 の対象 2 3 2 2 のフィールドには、処理を実行する装置を特定する情報が格納される。

【0054】

(変形例 6)

ゲートウェイ 2 0 は、通信を統括する機能である通信部 2 9 を有さなくてもよい。すなわちゲートウェイ 2 0 以外の装置に、ログ収集部 2 1、機能安全解析部 2 2 1、情報安全解析部 2 2 2、G W 記憶部 2 3、および決定部 2 4 の機能が搭載されてもよい。

【0055】

10

20

30

40

50

(変形例 7)

図 6 に示すように、ゲートウェイ 20 は、機能安全機能実行部 31、情報安全機能実行部 32、ECU 記憶部 33、および車両内ログ収集部 34 の機能を備えてもよい。この場合には、電子制御システム 1 は ECU 30 を含まなくてもよい。

【0056】

上述した実施の形態は、次の<1>～<4>のように変形してもよい。

<1>ログ収集部 21 が収集したセーフティログ 331 およびセキュリティログ 332 は、GW 記憶部 23 の代わりに、不図示の一時記憶部に格納されてもよい。

<2>ゲートウェイ 20 は、複数の装置からログを収集してもよい。

<3>ゲートウェイ 20 は、ログ収集部 21 を備えず、他の装置からログを受信する構成としてもよい。

<4>機能安全対処表 231 および情報安全対処表 232 は、一体に構成されてもよい。

【0057】

上述した各実施の形態および変形例において、機能ブロックの構成は一例に過ぎない。別々の機能ブロックとして示したいくつかの機能構成を一体に構成してもよいし、1つの機能ブロック図で表した構成を2以上の機能に分割してもよい。また各機能ブロックが有する機能の一部を他の機能ブロックが備える構成としてもよい。

【0058】

上述した各実施の形態および変形例において、プログラムは不図示のROMに格納されたとしたが、プログラムは不揮発性メモリに格納されていてもよい。また、ゲートウェイ 20 および不図示の入出力インタフェースを備え、必要なときに入出力インタフェースとゲートウェイ 20 が利用可能な媒体を介して、他の装置からプログラムが読み込まれてもよい。ここで媒体とは、例えば入出力インタフェースに着脱可能な記憶媒体、または通信媒体、すなわち有線、無線、光などのネットワーク、または当該ネットワークを伝搬する搬送波やデジタル信号、を指す。また、プログラムにより実現される機能の一部または全部がハードウェア回路やFPGAにより実現されてもよい。

【0059】

上述した各実施の形態および変形例は、それぞれ組み合わせてもよい。上記では、種々の実施の形態および変形例を説明したが、本発明はこれらの内容に限定されるものではない。本発明の技術的思想の範囲内で考えられるその他の態様も本発明の範囲内に含まれる。

【符号の説明】

【0060】

- 1 … 電子制御システム
- 20 … ゲートウェイ
- 21 … ログ収集部
- 23 … GW 記憶部
- 24 … 決定部
- 29 … 通信部
- 31 … 機能安全機能実行部、セーフティ機能実行部
- 32 … 情報安全機能実行部、セキュリティ機能実行部
- 33 … ECU 記憶部
- 34 … 車両内ログ収集部
- 121 … セキュリティログ
- 122 … セーフティログ
- 221 … 機能安全解析部、セーフティイベント解析部
- 222 … 情報安全解析部、セキュリティイベント解析部
- 231 … 機能安全対処表
- 232 … 情報安全対処表
- 233 … 対処表
- 331 … セーフティログ

10

20

30

40

50

3 3 2 …セキュリティログ
【図面】
【図 1】

【図 2】

図 1

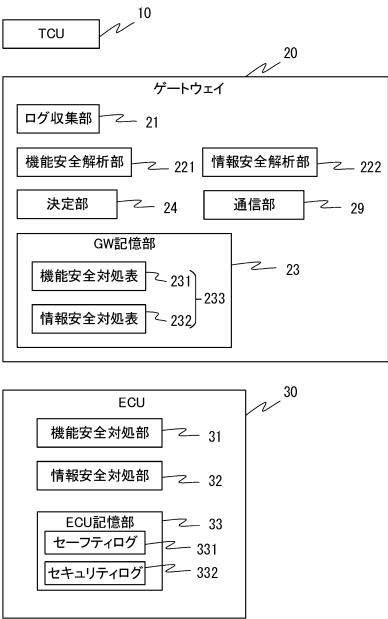


図2

機能安全対処表			
イベントID	対象	種別	対処
P1	ECU	セーフティ	E1
P2	ECU	セーフティ	E2
P3	ゲートウェイ	セーフティ	E3
.	.	.	.

10

20

30

40

50

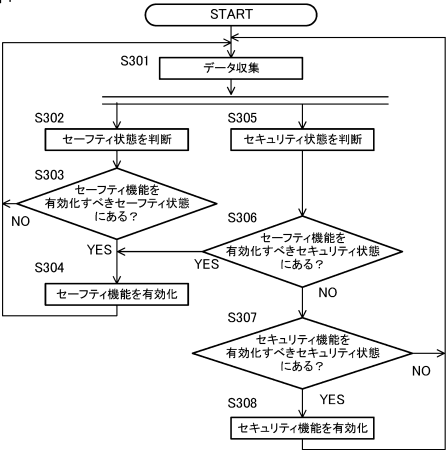
【図 3】

図3

情報安全対処表			
イベントID	対象	種別	対処
Q1	ECU	セキュリティ	F1
Q2	ECU	セーフティ	E5
Q3	ECU	セーフティ	E2
.	.	セキュリティ	F2

【図 4】

図4

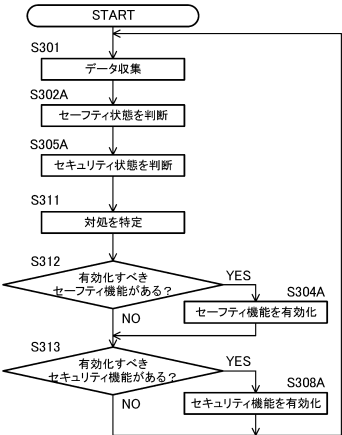


10

20

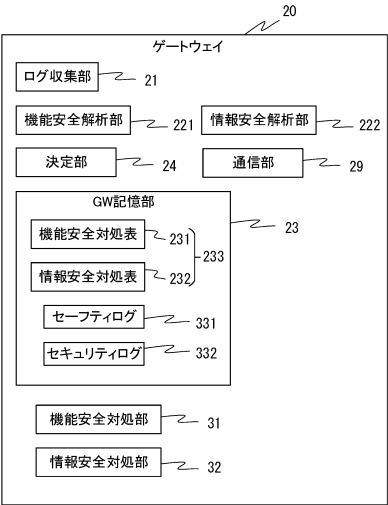
【図 5】

図5



【図 6】

図6



30

40

50

フロントページの続き

- (56)参考文献 国際公開第2015/001594 (WO, A1)
特開2019-073102 (JP, A)
特開2019-205125 (JP, A)
特開2017-152762 (JP, A)
- (58)調査した分野 (Int.Cl., DB名)
G06F 21/55
G05B 19/048
G05B 9/02