【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】平成30年1月25日(2018.1.25)

【公開番号】特開2016-19280(P2016-19280A)
【公開日】平成28年2月1日(2016.2.1)
【年通号数】公開・登録公報2016-007
【出願番号】特願2014-243828(P2014-243828)
【国際特許分類】
Ｈ０４Ｌ　9/32　(2006.01)
Ｇ０９Ｃ　1/00　(2006.01)
Ｇ０５Ｂ　9/03　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６７５Ｂ
Ｇ０９Ｃ　1/00　６４０Ｅ
Ｇ０５Ｂ　9/03

【手続補正書】
【提出日】平成29年12月4日(2017.12.4)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
安全な産業制御システムであって、
１つ以上の産業用エレメントと、
１つ以上の産業用エレメントを駆動する一組の冗長な通信／制御モジュールと、
を備え、
冗長な通信／制御モジュールのセットは、認証シーケンスを実行するために構成される第１通信／制御モジュールおよび第２通信／制御モジュールを含み、
認証シーケンスが、
第１通信／制御モジュールから第２通信／制御モジュールまでリクエスト・データグラムを送信するステップであって、リクエスト・データグラムが、第１ノンスと、第１デバイス認証キー証明書と、第１アイデンティティ属性証明書とを含む、ステップと、
第２通信／制御モジュールから第１通信／制御モジュールまで応答データグラムを送信するステップであって、応答データグラムが、第２ノンスと、第１および第２ノンスに関連した第１シグニチャーと、第２デバイス認証キー証明書と、第２アイデンティティ属性証明書とを含む、ステップと、
応答データグラムが有効であるとき、第１通信／制御モジュールから第２通信／制御モジュールまで認証データグラムを送信するステップであって、認証データグラムが第１および第２ノンスに関連した第２シグニチャーを含む、ステップと、
を有する、安全な産業制御システム。
【請求項２】
第１および第２通信／制御モジュールにより実行される認証シーケンスが、更に、
応答データグラムが無効であるとき、第１通信／制御モジュールから第２通信／制御モジュールまで失敗した認証データグラムを送信するステップを有し、
失敗した認証データグラムが、第２ノンスに関連したシグニチャーと、第１通信／制御モジュールにより生成されるエラー・メッセージとを含む、請求項１に記載の安全な産業

制御システム。
【請求項３】
第１および第２通信／制御モジュールにより実行される認証シーケンスが、更に、
第２通信／制御モジュールから第１通信／制御モジュールまで応答する認証データグラムを送信するステップを有し、
応答する認証データグラムは、第１ノンスに関連したシグニチャーと、第２通信／制御モジュールにより生成される成功または失敗メッセージとを含む、請求項１に記載の安全な産業制御システム。
【請求項４】
第１ノンスおよび第２ノンスの少なくとも１つが、真性乱数発生器により生成されるランダムなノンスを含む、請求項１に記載の安全な産業制御システム。
【請求項５】
第２通信／制御モジュールが、第１ノンスおよび第２ノンスを連結し、第１ノンスおよび第２ノンスの連結に署名することによって、第１および第２ノンスに関連した第１シグニチャーを生成するように構成され、
第１通信／制御モジュールが、第１ノンスおよび第２ノンスを連結し、第１ノンスおよび第２ノンスの連結に署名することによって、第１および第２ノンスに関連した第２シグニチャーを生成するように構成される、請求項１に記載の安全な産業制御システム。
【請求項６】
第２通信／制御モジュールが、更に、第１デバイス認証キー証明書および第１アイデンティティ属性証明書を検査することによって、リクエスト・データグラムを確認するように構成される、請求項１に記載の安全な産業制御システム。
【請求項７】
第１通信／制御モジュールが、更に、第１および第２ノンスに関連した第１シグニチャー、第２デバイス認証キー証明書、および第２アイデンティティ属性証明書を検査することによって、応答データグラムを確認するように構成される、請求項１に記載の安全な産業制御システム。
【請求項８】
第１通信／制御モジュールが、第１ノンスおよび第２ノンスを連結することによって、パブリック・デバイス認証キーを用いて第１および第２ノンスに関連した第１シグニチャーを暗号により検査することによって、並びに、第１ノンスおよび第２ノンスについてローカルに生成された連結を、第１ノンスおよび第２ノンスについて暗号により検査された連結と比較することによって、第１および第２ノンスに関連した第１シグニチャーを検査するように構成される、請求項７に記載の安全な産業制御システム。
【請求項９】
第２通信／制御モジュールが、第１通信／制御モジュールから認証データグラムを受け取ることに応答して、第１ノンスおよび第２ノンスを連結することによって、パブリック・デバイス認証キーを用いて第１および第２ノンスに関連した第２シグニチャーを暗号により検査することによって、並びに、第１ノンスおよび第２ノンスについてローカルに生成された連結を、第１ノンスおよび第２ノンスについて暗号により検査された連結と比較することによって、第１および第２ノンスに関連した第２シグニチャーを検査するように構成される、請求項１に記載の安全な産業制御システム。
【請求項１０】
第１および第２通信／制御モジュールが、スタートアップ／リセット・イベント、第１通信／制御モジュールまたは第２通信／制御モジュールの設置、周期的時間イベント、または、予定の時間イベントの内の少なくとも１つに応答して認証シーケンスを実行するように構成される、請求項１に記載の安全な産業制御システム。
【請求項１１】
１つ以上の産業用エレメントが、入出力モジュール、パワー・モジュール、フィールド・デバイス、スイッチ、ワークステーション、または、物理的な相互接続デバイスの内の

少なくとも１つを含む、請求項１に記載の安全な産業制御システム。
【請求項１２】
通信／制御モジュールであって、
少なくとも１つのプロセッサと、
少なくとも１つのプロセッサによって、実行可能な命令のセットを有する非一時的な媒体とを有し、
命令のセットが、
第１ノンスと、第１デバイス認証キー証明書と、第１アイデンティティ属性証明書と、を含むリクエスト・データグラムを、第２通信／制御モジュールに送らせ、
第２ノンスと、第１および第２ノンスに関連した第１シグニチャーと、第２デバイス認証キー証明書と、第２アイデンティティ属性証明書とを含む応答データグラムを、第２通信／制御モジュールから受け取らせ、
応答データグラムが有効であるとき、第１および第２ノンスに関連する第２シグニチャーを含む認証データグラムを、第２通信／制御モジュールに送らせる、
命令を含む、通信／制御モジュール。
【請求項１３】
命令のセットが、更に、
応答データグラムが無効であるとき、第２ノンスに関連したシグニチャーと、エラー・メッセージとを含む失敗した認証データグラムを、第２通信／制御モジュールに送らせる命令を含む、請求項１２に記載の通信／制御モジュール。
【請求項１４】
命令のセットが、更に、
第１および第２ノンスに関連した第１シグニチャーと、第２デバイス認証キー証明書と、第２アイデンティティ属性証明書とを検査することによって、応答データグラムを確認させる命令を含む、請求項１２に記載の通信／制御モジュール。
【請求項１５】
命令のセットが、更に、
第１ノンスおよび第２ノンスを連結することによって、パブリック・デバイス認証キーを用いて第１および第２ノンスに関連した第１シグニチャーを暗号により検査することによって、並びに、第１ノンスおよび第２ノンスについてローカルに生成された連結を、第１ノンスおよび第２ノンスについて暗号により検査された連結と比較することによって、第１および第２ノンスに関連した第１シグニチャーを検査させる命令を含む、請求項１４に記載の通信／制御モジュール。
【請求項１６】
通信／制御モジュールであって、
少なくとも１つのプロセッサと、
少なくとも１つのプロセッサによって実行可能な命令のセットを有する非一時的な媒体とを備え、
命令のセットが、
第１ノンスと、第１デバイス認証キー証明書と、第１アイデンティティ属性証明書とを含むリクエスト・データグラムを、第２通信／制御モジュールから受け取らせ、
第２ノンスと、第１および第２ノンスに関連する第１シグニチャーと、第２デバイス認証キー証明書と、第２アイデンティティ属性証明書とを含む応答データグラムを、該応答データグラムが有効であるときに、第２通信／制御モジュールに送らせる、
命令を含む、通信／制御モジュール。
【請求項１７】
命令のセットが、更に、
第１および第２ノンスに関連する第２シグニチャーを含む認証データグラムを、第２通信／制御モジュールから受け取らせ、
第１ノンスに関連するシグニチャーと、成功または失敗メッセージとを含む、応答する

認証データグラムを第２通信／制御モジュールに送らせる、
命令を含む、請求項１６に記載の通信／制御モジュール。
【請求項１８】
命令のセットが、更に、
第１ノンスおよび第２ノンスを連結することによって、パブリック・デバイス認証キーを用いて第１および第２ノンスに関連した第２シグニチャーを暗号により検査することによって、並びに、第１ノンスおよび第２ノンスについてローカルに生成された連結を、第１ノンスおよび第２ノンスについて暗号により検査された連結と比較することによって、第１および第２ノンスに関連した第２シグニチャーを検査させる命令を含む、請求項１７に記載の通信／制御モジュール。
【請求項１９】
命令のセットが、更に、
第１ノンスおよび第２ノンスを連結することによって、並びに、第１ノンスおよび第２ノンスの連結に署名することによって、第１および第２ノンスに関連した第１シグニチャーを生成させる命令を含む、請求項１６に記載の通信／制御モジュール。
【請求項２０】
命令のセットが、更に、
第１デバイス認証キー証明書および第１アイデンティティ属性証明書を検査することによって、リクエスト・データグラムを確認させる命令を含む、請求項１６に記載の通信／制御モジュール。