(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第5406013号
(P5406013)

(45)発行日　平成26年2月5日(2014.2.5)　(24)登録日　平成25年11月8日(2013.11.8)

(51)Int.Cl.		F I		
H04L 9/32	(2006.01)	H04L	9/00	675A
G09C 1/00	(2006.01)	G09C	1/00	660E
G06F 21/44	(2013.01)	G06F	21/20	144A

請求項の数 11　(全 10 頁)

(21)出願番号	特願2009-505744 (P2009-505744)
(86)(22)出願日	平成19年4月5日(2007.4.5)
(65)公表番号	特表2009-534697 (P2009-534697A)
(43)公表日	平成21年9月24日(2009.9.24)
(86)国際出願番号	PCT/EP2007/003101
(87)国際公開番号	WO2007/121844
(87)国際公開日	平成19年11月1日(2007.11.1)
審査請求日	平成22年3月10日(2010.3.10)
(31)優先権主張番号	0603378
(32)優先日	平成18年4月18日(2006.4.18)
(33)優先権主張国	フランス(FR)

(73)特許権者　509347273
エアバス　オペラシオン　ソシエテ　パ
アクシオンス　シンプリフィエ
フランス国，エフ－３１０６０　トゥールズ，ルート　ド　ベイヨンヌ　３１６
(74)代理人　100099759
弁理士　青木　篤
(74)代理人　100092624
弁理士　鶴田　準一
(74)代理人　100122965
弁理士　水谷　好男
(74)代理人　100141162
弁理士　森　啓

最終頁に続く

(54)【発明の名称】航空機と地上局との間の通信ネットワーク上の通信方法と装置

(57)【特許請求の範囲】

【請求項１】

航空機と地上局との間の通信ネットワーク（１２）上の通信方法であって、

前記通信ネットワークは複数のセキュリティレベルにより構成されており、

航空機が通信セキュリティレベルを旧セキュリティレベルから新セキュリティレベルに変更する要請を地上局に送り、前記要請の地上局の受信確認応答を受信しないときに、前記航空機は新セキュリティレベルで地上局から送られてきたメッセージを受け取ることを特徴とする通信方法。

【請求項２】

前記航空機が前記受信確認応答を受信せず、新セキュリティレベルが旧セキュリティレベルより高い場合、航空機は地上局から送られたメッセージを旧セキュリティレベルで受け取ることを特徴とする請求項１に記載の通信方法。

【請求項３】

前記航空機が前記受信確認応答を受信せず、新セキュリティレベルが旧セキュリティレベルより高い場合、航空機は、セキュリティレベル変更に関する前記地上局の受信確認応答を受信しない間は、地上局へ旧セキュリティレベルでメッセージを送信することを継続することを特徴とする請求項１又は２に記載の通信方法。

【請求項４】

航空機がセキュリティレベルの変更に関する地上局の受信確認応答を受信せず、新セキュリティレベルが旧セキュリティレベルより低い場合、航空機は旧セキュリティレベルで

地上局から受信するメッセージを拒否することを特徴とする請求項１に記載の通信方法。
【請求項５】
航空機がセキュリティレベルの変更に関する地上局の受信確認応答を受信せず、新セキュリティレベルが旧セキュリティレベルより低い場合、航空機は地上局に新セキュリティレベルでメッセージを送信することを特徴とする請求項１又は４に記載の通信方法。
【請求項６】
航空機が地上局から前記新セキュリティレベルに対応するセキュリティレベルのメッセージを受信したとき、航空機において、通信セキュリティレベルの前記変更要請は地上局が受信確認したとする請求項１に記載の通信方法。
【請求項７】
前記通信セキュリティレベルは送信メッセージタイプにより変わることを特徴とする請求項１乃至６のいずれか１項に記載の通信方法。
【請求項８】
通信が、ハッカー攻撃のリスクに対する前記通信セキュリティの欠如に対応する第１セキュリティレベル、メッセージ送信者の認証に対応する第２セキュリティレベル、又はメッセージ送信者の認証並びにデータリンク１２に送信される送信メッセージの暗号化に対応する第３セキュリティレベルから構成されていることを特徴とする請求項１乃至７の何れか一項に記載の通信方法。
【請求項９】
通信が複数のセキュリティレベルにより構成されている、航空機と地上局との間の通信ネットワーク（１２）上の通信装置（１）であって、
通信ネットワーク（１２）上でメッセージの送受信する送受信手段（１０）と、
前記送受信手段（１０）に接続する通信制御手段（１４）と、
前記送受信手段により受信されるメッセージを解析し、同メッセージに対応するセキュリティレベルを決定する第１手段（２２）を含む通信監視手段（１６）と、
前記航空機が通信セキュリティレベルの変更要請を地上局に送信するときに新旧セキュリティレベルを記憶することのできる記憶手段と、
航空機から地上局に送信された通信のセキュリティレベルの変更要請の地上局の受信確認応答又は受信確認応答の不存在に対応する通信状態を記憶することの出来る記憶手段と、
を備え、
前記通信監視手段（１６）は、
該受信メッセージに対応する前記セキュリティレベルを前記記憶された新セキュリティレベルと比較し、比較結果を出力することのできる第２手段と、
前記第２手段（２４）から出力される比較結果（第１部分）及び記憶されている通信状態値（第２部分）に応じて前記受信メッセージの受取りに関係する動作を決定することの出来る第３手段（２６）と、
を有し、
前記送受信手段は、航空機が通信セキュリティレベルを旧セキュリティレベルから新セキュリティレベルに変更する要請を地上局に送り、前記要請の地上局の受信確認応答を受信しないときに、前記航空機は新セキュリティレベルで地上局から送られてきたメッセージを受け取ることを特徴とする通信装置。
【請求項１０】
請求項１乃至８の何れか一項に記載の方法を実施することのできる装置を備える航空機。
【請求項１１】
請求項９に記載の通信装置（１）を備える航空機。
【発明の詳細な説明】
【技術分野】
【０００１】

本発明は航空機と地上局との間の安全化された通信ネットワーク上の通信方法を対象とする。特に本通信に関係するセキュリティレベルを変更するときの通信方法を対象とする。又、本方法を実行することのできる装置を有する航空機に関する。同様に、本発明は航空機と地上局との間の安全化された通信ネットワーク上の通信装置に関する。特に本通信に関係するセキュリティレベルを変更するときの通信装置に関する。又、本装置を有する航空機に関する。

【背景技術】

【０００２】

最近の航空機、特に民生用輸送機は、地上局、特に管制局又は航空機開発会社との交信を可能にする局と情報の交信を行っている。交信される情報は特に気象、航空機のメンテナンス、航行管制の許可等に関する。この情報交信は一般的に特にＡＣＡＲＳ（Aircraft Communications Adressing and Reporting System）又はＡＴＮ（Aeronautical Telecommunication Network）に対応するデータリンクを使って実行されている。一般的に、これらデータリンクは無線通信又は衛星を使うタイプである。ハッカー侵入のリスクを考慮して、交信データの秘密及び通信セキュリティを保証するために、これらデータリンクは安全化されることができる；このため、例えば、メッセージ送信者の認証及び/又はメッセージの暗号化を行うことができる。このセキュリティレベルは航空機パイロットにより選択されている。この認証及び/又は暗号化は、例えば、認証キー及び/又は暗号化キーを使って実行されている。

【発明の開示】

【発明が解決しようとする課題】

【０００３】

しばしば、航空機の飛行中に通信のセキュリティレベルを変更させることが必要になる。特に暗号化通信を禁止している国を飛行する時にはそうである。航空機のパイロットが通信セキュリティレベルの変更を要求するときに、もし航空機が地上局に対しセキュリティレベルの変更を要請し、地上局がこの要請に受信確認応答をしない時、航空機の要求レベル（新規レベル）と地上局により動作されていると認識されているセキュリティレベル（旧レベル）とは一致しなくなる。特に、地上局からの、上記要請の受信確認応答がないことは、航空機から地上局に対して送られる要求メッセージの消失したこと又は、航空機に対し地上局から送られた前記受信確認応答メッセージが消失したことが原因である可能性がある。

【０００４】

通信分野における、送信者と受信者の間の不一致（incoherence）状態を改善するための従来方法は、送信者と受信者の通信を初期状態からやり直すことであった。対象の通信ネットワークにおいて、非安全化通信状態から航空機と地上局との間の通信を再初期化し、所望のセキュリティレベルに対応するセキュリティレベルを使って安全化通信セッションを開始することができる。しかしながら、この方法では不都合なことが多い。第１の不都合は航空機と地上局との間で安全化通信セッションを再開するためには航空機と地上局との間で複数のメッセージを交信することが必要である。従って、前記セッション確立の時間が必要であり、これを無視することは出来ない。これは航空機と地上局との間の通信の必要性から見て不利益である可能性がある。というのは前記セッション確立の期間、航空機と地上局は有用なメッセージを交信できないからである。

第２の不都合は、安全化されていない初期の通信状態に戻ることは通信セキュリティに損害を与える可能性があるという事実に関係する。特に仮にメッセージが、通信が非安全化通信状態で再初期化される時点と安全化されたセッションの開始時点の間で、航空機と地上局との間で交信される場合はそうである。

【課題を解決するための手段】

【０００５】

航空機と地上局との間の通信ネットワーク上での本発明の通信方法によれば、これらの問題は少なくとも部分的には、解決される。前記通信ネットワークは複数のセキュリティ

レベルにより構成されることができ、航空機が通信セキュリティレベルを旧セキュリティレベルから新セキュリティレベルに変更する要請を地上局に送り、航空機が地上局による前記要請の受信確認応答（acquittement）を受信しないときでも、前記航空機は新セキュリティレベルで地上局から送られてきたメッセージを受け取ることを特徴とする。

【０００６】

このように、仮に地上局が航空機の送信したセキュリティレベル変更要請を受信し処理したが、地上局から送られた受信確認応答メッセージが航空機により受信されなかった場合でも、望まれたセキュリティレベルでの通信を継続することが保証される。

【０００７】

好ましい実施例において、航空機がセキュリティレベルの変更に関する地上局の受信確認応答（acquittement）を受信しなかったという条件で：

新セキュリティレベルが旧セキュリティレベルより低い場合、航空機は旧セキュリティレベルで地上局から送信されたメッセージを拒否する；

新セキュリティレベルが旧セキュリティレベルより高い場合、航空機は旧セキュリティレベルで地上局にメッセージを送信し続ける；

新セキュリティレベルが旧セキュリティレベルより低い場合、航空機は地上局に新セキュリティレベルでメッセージを送信する。

航空機のパイロットが通信の暗号化を禁止する国の上空を通過するために通信のセキュリティレベルを下げるように要求するとき、本発明の好ましい実施例によれば、上空を通過する国の法令を尊重することができる。

【０００８】

新セキュリティレベルが旧セキュリティレベルより高い場合、航空機がセキュリティレベル変更に関する地上局の受信確認応答を受信しない間は、旧セキュリティレベルで地上局から送信されたメッセージを受取ることが有利である。

【０００９】

本発明の特別の実施例において、通信のセキュリティレベルは送信メッセージタイプにより変わる。これにより、メッセージの重要性（importance）と重大性(criticite)のレベルに適合させ、重要性を示すメッセージだけを高いセキュリティレベル（低いセキュリティレベルで送信するより送信コストが高い）で送信することができる。

【００１０】

本発明の別の特別な実施例において、航空機が前記新セキュリティレベルに対応するセキュリティレベルのメッセージを地上局から受信したとき、航空機側では、通信のセキュリティレベルの前記変更要請についての、地上局による受信確認応答があったと考えられる。実際、地上局は新セキュリティレベルでメッセージを送信したのであるから、地上局は航空機から送信されたセキュリティレベル変更要請を考慮したと考えることができる：航空機が受信する前記メッセージの地上局による送信は、上記要請の明示的ではない受信確認応答に相当する。これにより航空機が要求するセキュリティレベル（新レベル）と地上局が動作している（actif）として認識している現状レベルとの一致状態に復帰することが可能になる。

【００１１】

また、本発明は、航空機と地上局との間の通信ネットワーク上の上記通信方法を実施することのできる航空機に関する。

【００１２】

同様に、本発明は航空機と地上局との間の通信ネットワーク上の通信装置に関する。なお、前記通信は複数のセキュリティレベルに基づいて構成でき、次の手段を有している；

【００１３】

― 通信ネットワーク上でメッセージを送受信する送受信手段；

― 前記送受信手段に接続している通信制御手段；

― 前記送受信手段により受信されたメッセージを解析し、同メッセージに対応するセキュリティレベルを決定する第１手段を含む通信監視手段；

【００１４】
更に、上記装置は次の手段を有するという特徴がある：
― 航空機が通信セキュリティレベルの変更要請を地上局に送信するときに新旧セキュリティレベルを記憶する記憶手段；
― 航空機から地上局に送信された通信のセキュリティレベルの変更要請を地上局が受信確認応答又は受信確認応答の欠如に対応する通信状態を記憶することが出来る記憶手段；
【００１５】
― 通信監視手段において:
― 該受信メッセージに対応する前記セキュリティレベルと記憶された前記新セキュリティレベルとを比較し、比較結果を出力することのできる第２手段；
― 前記第２手段から出力される比較結果（第１部分）及び記憶された通信状態値（第２部分）に応じて受信された前記メッセージの受取りに関係する動作を決定することの出来る第３手段。
【００１６】
前記通信制御手段が前記通信監視手段を有すると有利である。
【００１７】
更に、前記通信制御手段は前記ネットワークに関係する通信状態値を制御することのできる手段を有すると有利である。
【００１８】
また、本発明は航空機と地上局との間の通信を行う通信装置を備える航空機に関する。
【００１９】
本発明は以下の説明を読み、図面を参照することにより、理解を進めることができる。
【発明を実施するための最良の形態】
【００２０】
図１は本発明に基づく、航空機と地上局との間の通信ネットワーク上で通信を行う通信装置のブロック図である。
【００２１】
本発明に基づく装置１は、図１に示されるように、航空機に、特に民間輸送機に搭載されている。同航空機は、通信ネットワーク１２を用いて、具体的にはデジタルデータネットワーク(データリンク)を用いて地上局と通信を行う。このネットワークはハッカー侵入のリスクに対し、複数のセキュリティレベルに基づいて構成されている。
【００２２】
特に航空機が要求するセキュリティレベルと地上局が動作していると認識しているセキュリティレベルとの間に不一致がある時に、前記装置は、前記ネットワーク１２上で航空機により受信されるメッセージを受取る又は拒否するかを決定するように設計されている。そのために、本発明による装置１は次の手段を備えている。
【００２３】
― 前記航空機と前記地上局との間の通信ネットワーク（例えば、前記航空機に搭載された通常の通信手段〔ＶＨＦ,ＨＦ無線通信手段、衛星通信手段等〕）１２上でメッセージを送受信する送受信装置１０；
― ネットワーク３０を介して前記送受信手段１０に接続されている複数の通信制御手段１４；
― 航空機が通信のセキュリティレベルの変更を地上局に送信するとき、新旧のセキュリティレベルを記憶することが出来る記憶手段（図示しない）。これら手段は通信制御手段の一部分を構成することが好ましい；
― 航空機が地上局に向けて送信した通信セキュリティレベルの変更要請に対する地上局による受信確認応答又は受信確認応答の不存在に対応する通信状態を記憶することのできる記憶手段２８；
【００２４】
― 通信監視手段１６、該通信監視手段は以下を備えている；

― 前記送受信手段により受信されるメッセージを解析し、メッセージに対応するセキュリティレベルを決定する第１手段２２；
―前記受信メッセージに対応するセキュリティレベルと記憶された新しい前記セキュリティレベルとを比較し、比較結果を出力する第２手段２４；
― 前記第２手段２４から出力される比較結果、及び、前記記憶された前記通信状態値に応じて前記受信メッセージの受取りに関係する動作を決定する第３手段２６。

【００２５】

前記通信制御手段１４は、通信ネットワーク１２、送受信手段１０、ネットワーク３０を介してメッセージを受信し、各メッセージをネットワーク３４を介して少なくとも１つの送信先アプリケーションＡ１，Ａ２、…Ａｎに送信するルータ１８を備えることが好ましい。前記各アプリケーションは特に航空機の計算機にインストールされるコンピュータアプリケーションである。同様に、該ルータはネットワーク３４を介して前記アプリケーションから来るメッセージを収集し、送受信装置１０を使ってネットワーク３０を介して送信する。同送信／受信装置１０は通信ネットワーク１２上にそれらを送信する。

【００２６】

更に、図１に示すように、通信監視手段１６は通信制御手段１４に組み込まれていることが好ましい。通信監視手段はネットワーク３２を介してルータ１８に接続している。

【００２７】

更に、通信制御手段１４は通信ネットワーク１２の通信状態を制御する手段２８を備えている。同手段２８は特に通信監視手段１６に組み込まれている。これら手段２８は少なくとも２つの状態を含むマシーン状態（machine d’etat）に対応する：第１状態は航空機が要求するセキュリティレベルと地上局が動作していると認識しているセキュリティレベルとの間の一致に対応する。また、第２状態は航空機が要求するセキュリティレベルと地上局が動作していると認識しているセキュリティレベルとの間の不一致に対応する。

【００２８】

この第２状態は、特に、通信のセキュリティレベルを変更するために（例えば、航空機のパイロットの要請(demande)の後で）航空機の通信制御手段１４が地上局宛に要請メッセージを送信したが、航空機の前記通信制御手段１４が該セキュリティレベルの変更に関する地上局の受信確認応答を受信しなかった状態、に対応する。もし航空機が通信のセキュリティレベルの変更の要請を地上局に送信した後で地上局の受信確認応答を受信していない場合、航空機は所定時間経過後に再度、地上局に前記要請を送信することが好ましい。

【００２９】

航空機は少なくとも所定回数Ｎ（例えば３回）この要請を地上局に送信することができる。前記第２状態は、Ｎ回のセキュリティレベルの変更要請を地上局の受信確認応答を航空機が受信しなったときだけ実行される。

これにより、受信確認応答の受信の不存在が通信ネットワークの短期間の外乱、例えば、電磁的外乱に起因するという状況から解放されることができる。

【００３０】

これに対し、第１状態は、特に航空機の通信制御手段１４が、通信のセキュリティレベルを変更するために（例えば、航空機のパイロットの要請(demande)の後で）地上局宛に要請メッセージを送信した後で、前記セキュリティレベルの変更に関係する地上局の受信確認応答を受信した状態、に対応する：航空機が要求するセキュリティレベルと地上局が認識しているセキュリティレベルとが一致している。

【００３１】

通信制御手段１４がＡＴＳＵタイプ計算機の一部を構成している場合、通信制御手段１４に備えられている通信監視手段１６（同様に、第１手段２２、第２手段２４、第３手段２６、及び、通信状態を制御できる手段２８）は前記ＡＴＳＵ計算機のソフトウェアの形で実施されることができる。

【００３２】

特に、通信のセキュリティレベルは次のセキュリティレベル全体又はその下位のセキュリティレベルから選択される：
－ハッカー攻撃のリスクに対する通信セキュリティの欠如；
－メッセージ送信者の認証（例えば、認証キーを使う認証アルゴリズムを使う）；
－データリンク１２における送信メッセージの暗号化（例えば、暗号キーを使う認証アルゴリズムを使う）；
－送信メッセージの送信者の認証、及び、データリンク１２における送信メッセージの暗号化。

【００３３】

本発明の好ましい実施例において、通信は次のように構成される。
－ハッカー攻撃のリスクに対する通信セキュリティの欠如に対応する第１セキュリティレベル；
－メッセージ送信者の認証に対応する第２セキュリティレベル；又は、
－メッセージ送信者の認証、且つ、データリンク１２における送信メッセージの暗号化に対応する第３セキュリティレベル。

【００３４】

前記送受信手段１０は通信ネットワーク１２からメッセージを受信するとき、ネットワーク３０を介して通信制御手段１４にそれを送信する。通信制御手段１４では同メッセージはルータ１８により受信される。後者はそれを複数の通信監視手段１６に組み込まれている複数の第１手段２２に、ネットワーク３２を介して送信する。これら第１手段２２は該メッセージを分析し、同メッセージに対応するセキュリティレベルを決定する。このセキュリティレベルはネットワーク３６を介して複数第２手段２４に送信される。前記第２手段はこのセキュリティレベルを通信のセキュリティレベル（通信制御手段１４に記憶されている）と比較する。受信メッセージのセキュリティレベルと通信のセキュリティレベルとの比較結果は、ネットワーク３８を介して第２手段２４により複数の第３手段２６に送信される。

【００３５】

第３手段２６は、ネットワーク４０を介して複数の手段２８から、通信ネットワーク１２に関係する前記通信状態を受信する。該通信状態が第１状態（航空機が要請するセキュリティレベルと地上局が動作していると認識しているセキュリティレベルとの間が一致している）である場合、従来のように、そのセキュリティレベルが新セキュリティレベルに対応するとき、第３手段２６はネットワーク３２を介してルータに、受信メッセージを受取ったという情報を送り返す。そのセキュリティレベルが新セキュリティレベルと異なるとき、第３手段２６は受信メッセージを拒否したという情報をネットワーク３２を介してルータに送り返す。前記通信状態が前記第２状態（航空機が要請するセキュリティレベルと地上局が動作していると認識しているセキュリティレベルとが不一致である）である場合、そのセキュリティレベルが新セキュリティレベルに一致するときに、第３手段２６はネットワーク３２を介してルータに受信メッセージの受取り情報を送り返す。この機能モードは有利である。何故なら、この場合には、航空機が要請するセキュリティレベルと地上局が動作していると認識しているセキュリティレベルとの間で一時的な不一致があるにも拘らず、安全化通信を継続することが可能であるからである。

【００３６】

ルータがネットワーク３２を介して受信メッセージの受取情報を受信するときには、全ネットワーク３４を介して送信先アプリケーションにこのメッセージを送信する。これに対し、ルータがネットワーク３２を介して受信メッセージの拒否情報を受信するときには、送信先アプリケーションにこのメッセージを送信しない。

【００３７】

前記第２手段２４は受信メッセージに対応するセキュリティレベルと通信制御手段１４に記憶されている旧セキュリティレベルとを比較することが好ましい。受信メッセージのセキュリティレベルと記憶されている旧セキュリティレベルとの比較結果は、ネットワー

ク３８を介して第２手段２４により第３手段２６に送信される。前記通信状態が前記第２状態（航空機が要請するセキュリティレベルと地上局が動作していると認識しているセキュリティレベルとが不一致である）に対応する場合は：

【００３８】

－そのセキュリティレベルと前記旧セキュリティレベルとの間が一致し、新セキュリティレベルが旧セキュリティレベルより高い場合には、第３手段２６はネットワーク３２を介して、受信メッセージの受取情報をルータに送り返す。この場合、航空機が要求するセキュリティレベルと地上局が動作していると認識しているセキュリティレベルとの間で一時的な不一致があるにも拘らず、安全化通信を継続することが可能である；

【００３９】

－そのセキュリティレベルと前記旧セキュリティレベルとの間が一致し、新セキュリティレベルが旧セキュリティレベルより低い場合には、第３手段２６はルータにネットワーク３２を介して、受信メッセージの拒否情報を送り返す。このようにすれば、航空機が要求する新セキュリティレベルより高いセキュリティレベルによって、航空機が地上局から送られたメッセージを受け取らないことが保証される。これにより、高いセキュリティレベル、特に通信暗号化を禁止する国の法規を遵守できる。

【００４０】

航空機が地上局にメッセージを送るとき、前記通信状態が前記第２状態（航空機が要請するセキュリティレベルと地上局が動作していると認識しているセキュリティレベルが一致していない）の場合、次のことが好ましい。

【００４１】

－ 新セキュリティレベルが旧セキュリティレベルより高いレベルの場合、複数の通信制御手段１４は、ネットワーク３０を介して送受信手段１０を用いて、更に通信ネットワーク１２を介して、旧セキュリティレベルに従って、このメッセージを地上局に送信する。これにより、旧セキュリティレベルによって安全化された通信を続行し、メッセージを地上局に送信することができる。航空機にとって、前記旧セキュリティレベルとは地上局が動作していると認識しているセキュリティレベルである。何故なら航空機はセキュリティレベル変更の要請についての受信確認応答を受信していないからである；

【００４２】

－ 新セキュリティレベルが旧セキュリティレベルより低い場合、複数の通信制御手段１４は、新セキュリティレベルによって、ネットワーク３０を介して複数の送受信手段１０を用いて、更に通信ネットワーク１２を介して前記メッセージを地上局に送信する。このようにすれば、航空機は、新セキュリティレベルより高いセキュリティレベルで地上局にメッセージを送ることはない。これにより、高いセキュリティレベル（特に通信暗号化）を禁止する国の法規を遵守できる。

【００４３】

前記通信状態が前記第２状態（航空機が要請するセキュリティレベルと地上局が動作していると認識しているセキュリティレベルが一致していない）の場合、次のことが好ましい。

【００４４】

－ 地上局から送られてくるメッセージを受信した後で、複数の通信制御手段１４は、ネットワーク３０、送受信手段１０、通信ネットワーク１２を介して要請メッセージを地上局に送信し、それを前記新セキュリティレベルにするために地上局に通信セキュリティレベル変更を再度要請する；及び/又は

【００４５】

－ 航空機が地上局にメッセージを送信する前に、複数の通信制御手段１４は、ネットワーク３０、送受信手段１０、通信ネットワーク１２を介して要請メッセージを地上局に送信し、それを前記新セキュリティレベルにするために地上局に通信セキュリティレベル変更を再度要請する。

【００４６】

航空機が要求するセキュリティレベルと地上局が動作していると認識しているセキュリティレベルとの間の一時的不一致をもたらす状況が消滅するならば、これによりこれらセキュリティレベルの一致を再度確立することができる。

【００４７】

本発明の第１の変形によれば、通信セキュリティレベルは、航空機と地上局との間の通信ネットワーク１２上で交信される全メッセージに共通している。

【００４８】

別の変形例によれば、前記通信ネットワーク上で交信されるメッセージがメッセージタイプに基づいてクラス分けされるとき、通信セキュリティレベルはメッセージタイプに応じて変わる。これには、セキュリティレベルをメッセージの重要性(importance)及び重大性（criticite）に適応させることができるという利点がある。従って、重要性であるメッセージだけを高いセキュリティレベル（例えば前記第３レベル）で送信することを可能にする。メッセージの送信コストがこのメッセージに対応するセキュリティレベルに応じて高くなるとき、航空機開発コストを低減させることが可能である。一例として、ＡＴＣ（Air Traffic Control）と呼ばれる第１メッセージタイプは航空機と航空管制との間で交信されるメッセージに対応することができる。又、ＡＯＣ（Air Operational Control）と呼ばれる第２メッセージタイプは航空機とこの航空機の開発会社との間で交信されるメッセージに対応することができる。

【図面の簡単な説明】

【００４９】

【図１】本発明に基づく、航空機と地上局との間の通信ネットワーク上で通信を行う通信装置のブロック図である。

【図１】

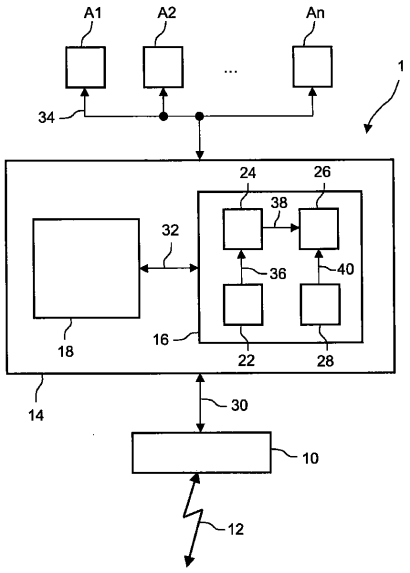

Fig. 1

フロントページの続き

(72)発明者 ルクレルク，アニエス
フランス国，エフ－３１５００ トゥールズ，リュ デュ ジェネラル トパン，２０
(72)発明者 コルーモルレク，セシル
フランス国，エフ－３１８６０ ラバルト シュール レズ，シュマン ドゥ テュロク，８９
(72)発明者 ブカール，パスカル
フランス国，エフ－３１７７０ コロミエ，アレ ドゥ ラ ジェリス，４

審査官 松平 英

(56)参考文献 特開平０３－０７０３２７（ＪＰ，Ａ）
特開昭６４－０６５９４５（ＪＰ，Ａ）
特開２００２－３００１６５（ＪＰ，Ａ）
特開２００４－０６４６５２（ＪＰ，Ａ）
特開２００５－１１７２３２（ＪＰ，Ａ）
特表２００９－５２９２６４（ＪＰ，Ａ）
国際公開第００／０７６１１７（WO，Ａ１）
特開平１０－２４２９５６（ＪＰ，Ａ）
特開平１１－２１５０３６（ＪＰ，Ａ）
特開２００４－０３２６６４（ＪＰ，Ａ）
特表２００１－５２２５４５（ＪＰ，Ａ）
特表２００２－５１１６９６（ＪＰ，Ａ）
特表２００５－５０２２４３（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ ９／００
Ｇ０９Ｃ １／００
Ｈ０４Ｌ １２／００
Ｈ０４Ｌ ２９／００
Ｈ０４Ｗ ４／００
Ｇ０６Ｆ ２１／２０
Ｇ０６Ｆ ２１／４４