自動運航船のセキュリティシステムアーキテクチャ

小林 英仁 [1,*]　松井 俊浩 [1]

概要：将来の自動運航船がセキュリティ上の脅威にさらされても安全に運航するためのゾーン型の自動操船システムアーキテクチャを提案する．外洋船の自動運航では，サイバーセキュリティの脅威にもさらされることから，目的地までの効率的な大域航路の計画のような上位タスクよりも悪天候回避，衝突回避，座礁回避，遠隔制御の実行，機関やリソースの保護，安全な接岸，安全な停船のような安全システムを強く保護する必要がある．これらは，多数のセンサと情報系，ソフトウェアをネットワークするが，安全システムは階層的に組み立てられるべきであることから，これらの情報系もゾーニングによって分離して安全を確保する必要がある．本稿では，これらの自動運航船の機能要求・安全要求を分析し，その実現に適したゾーニングアーキテクチャを提案する．

キーワード：自動運航船，自動操船システム，ゾーニング

Security System Architecture of Autonomous Ships

Hidehito Kobayashi[1,*]　Toshihiro Matsui[1]

Abstract: This paper proposes a zone-type automated ship maneuvering system architecture for safe operation even if future automatic ships are exposed to security threats. Since ocean-going vessels are also exposed to cybersecurity threats, they avoid bad weather, avoid collisions, avoid grounding, perform remote control, and perform higher-level tasks such as efficient global route planning to the destination. Safety systems such as engine and resource protection, safe berthing, and safe berths need to be strongly protected. These network many sensors, information systems, and software, but safety systems should be assembled hierarchically, so these information systems must also be separated and secured by zoning. In this paper, we analyze the functional requirements and safety requirements of these automatically operated ships and propose a zoning architecture suitable for the realization.

Keywords: Autonomous Ship, Ships Maneuvering System, Zoning

1. はじめに

海自業界では長年にわたり，年々高まる船員需要の逼迫や船員作業負担の増加等の課題に取り組むことが求められているが，特に近年の海上ブロードバンド技術やセンシング技術，AI，センシング技術，ビッグデータ技術等の急速な発展を受けて，自動運転技術を取り入れた船舶（自動運航船）の実現に大きな期待が寄せられている[1][2]．自動運航船の研究は 2012 年頃より特に欧州で勢力的に行われてきており，研究開発の初期には概念構築を目的としたプロジェクトが発足したが，実システムの構築や実証実験を行うものは見られなかった．しかし，2018 年 12 月には英海事大手ロールスロイス社らによって世界初の自律運航型フェリーが発表されるなど，近年になり研究成果が実社会のサービスとして現れつつある．

2. 関連研究

2.1 先行する自動運航船プロジェクト

自動運航船の研究開発プロジェクトとして，2025 年までにバルト海域での運航実現を目標とする One Sea プロジェクト（フィンランド）や電動無人運航コンテナ船の開発・建造及び就航を目指すプロジェクト（ノルウェー）をはじめ，主に無人コンテナ船の自動運航あるいは遠隔操船の実用化に向けたものが欧州を中心に多数進められているが，同研究開発分野において基礎となるシステムモデル及びリスクアセスメント結果を示したものとして，MUNIN（Maritime Navigation through Intelligence in Networks）プロジェクト[3]が挙げられる．同プロジェクトは，EU 支援のもとドイツや北欧諸国の大学・企業が共同し 2012 年から 2015 年にかけて実施された大規模プロジェクトである．その調査報告書[4]によれば，想定した運航シナリオの下で燃費が 10%以上向上するとともに，衝突・沈没に係るリスクが有人船と比較して 1 桁低くなることが示された．しかし，このプロジェクトでは安全上のリスクしか考慮されておらず，自動運航船のシステム（以下，自動操船システムと呼ぶ）の稼働環境の特殊性によりもたらされるサイバーセキュリティ上の脅威については十分な考察がなされていない．

Rødseth ら[5][6]は，MUNIN プロジェクトの自動操船システムモデルとして図 1 のような階層的モデルを発表した．上位層は高レベルの監視・制御機能を有し，下位層は船

1 情報セキュリティ大学院大学
Institute of Information Security

* mgs185505@iisec.ac.jp

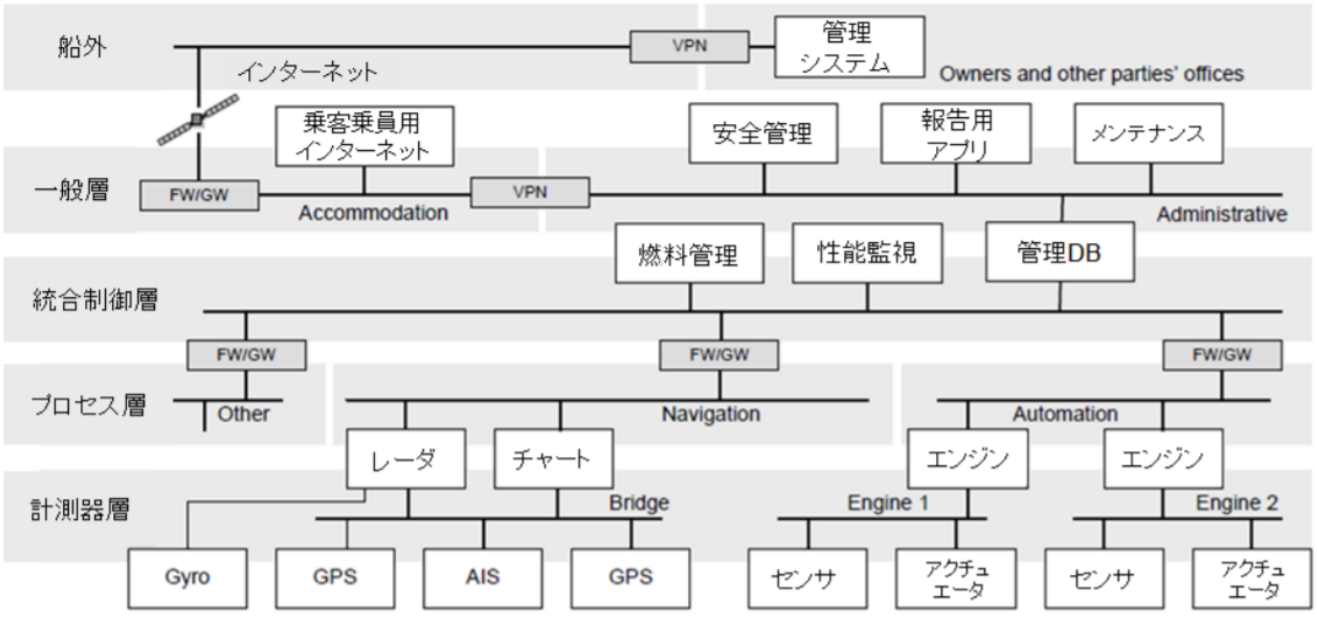

図 1　MUNIN プロジェクトで提案された自動操船システムモデル[5]

橋, エンジン, 安全機能等のプロセス毎に計測器を有する．各層はファイアウォール（FW）及びゲートウェイ（GW）で分離接続され，各層内の必要箇所において VPN による通信秘匿化が行われる．

Rødseth ら[7]は MUNIN プロジェクトにおけるリスクアセスメントの実施結果を発表したが，サイバーセキュリティ上の脅威について十分に考慮されているとは言えないものであった．

Wróbel ら[8]は，自動運航船における潜在的な事故要因（以下，ハザードと呼ぶ）を挙げ，各要因間の因果関係を分析することにより，あるハザードの発生が他のどのようなハザードの発生につながるかを分析するための枠組みを提案したが，サイバーセキュリティ上の脅威については扱われていない．

自動運航船の運用上のリスクを評価するにあたっては，操船システム稼動環境の特殊性を考慮した上で，安全面に限定したリスクアセスメントのみならずサイバーセキュリティ上の脅威分析も行うことが必要である．自動操船システムに対するサイバー攻撃のエントリポイントとして，(1)船内ネットワークとインターネットとをつなぐ衛星回線，(2)外部環境情報をセンシングする計測器群，及び(3)環境情報のセンシングを行わない, その他の機器群が挙げられる．

上記(1)の項目に関して，図 1 で船外と一般層との間の接続形態にみられるように，船内からインターネットへのアクセスは衛星回線経由となる．そのため，例えば船内システムの脆弱性修正プログラムの公開後，迅速にダウンロードするために最低限必要な通信速度の確保や回線障害に対する耐障害性対策等の検討が必要である．ただし，これらは工場やプラント等の制御システムや自動走行車においても同様の課題であり必ずしも自動操船分野だけにユニークな問題ではないことから，本稿ではこれ以上詳しく取り扱わないものとする．

上記(2)の項目に関して，これまで船内ネットワークを構成する個別機器の脆弱性が指摘されている．GPS 受信機に対する脅威としてジャミングやスプーフィング，ミーコニングがよく知られている．Humphreys[9]は実際の船舶を用いた実験において，GPS スプーフィングにより現在位置を偽装することで船舶が予定航路から逸脱する結果を示した．Bhatti ら[10]は正規の GPS 信号に微小な位置誤差を加えた信号を送ることで，海流の変化になりすまして偽装信号の検出を回避する手法及び同手法の対策を提案した．Balduzzi ら[11]は, 無線により他船の予定航路や目的地等の情報を受信するための機器である AIS（自動船舶識別装置）に関して，AIS 情報を偽装することにより船舶位置の偽装や架空の船舶の表示等が容易に行われることを示した．また船舶搭載機器としての直接的な考察はないものの，Petit ら[12]は自動走行車の LiDAR システムに対する距離偽装攻撃の評価実験結果を提示した．松本[13]は, 計測システムと計測対象それぞれに対するセキュリティ（計測セキュリティ）に係る脅威を体系的に分類し示した．Kimberly ら[14]は，操船システムに対するサイバー脅威を包括的かつ定量的に評価するためのフレームワークを提案した．

上記(3)の項目に関して，業務系ネットワークへの不正アクセスの防止措置の検討が不可欠である．図 1 の一般層にみられるように，自動操船システムにおいては乗客乗員用インターネット部と管理データベースや各種管理モジュール部とが同一ネットワーク内に混在することとなると考えられる．エンタープライズ系ネットワークと業務系ネットワークとを分離するための根本的な解決策は，両者の船外アクセス回線を別個に用意することであるが，回線調達・

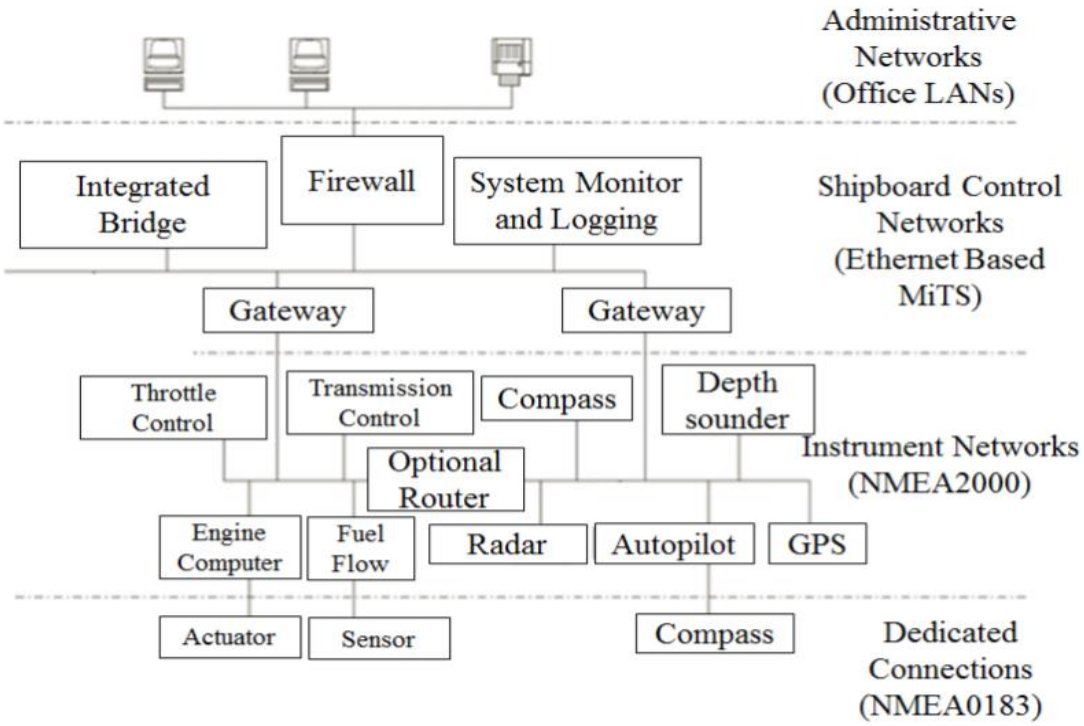

図 2 従来船における船内ネットワーク構成例[15]

維持管理に要するコストが制約となる場合がある．そのような場合には，ソフトウェア的解決手段として FW による不正アクセスの検出・遮断を行うほか，一般乗客が不用意に業務系ネットワークに接続することができないよう船員区画等へ入ることを禁止するというような物理的セキュリティの強化による解決が必要となる．

2.2 従来船における操船システムモデル例

図 2 は，船橋や通信室など船内の各区画に設置された機器を階層的に接続するとともに，衛星通信を介して陸上オフィスからそれらの機器にアクセスすることを想定して構成された船内ネットワークの例[15]である．同ネットワークは現行の舶用搭載機器の多くで採用されている NMEA と呼ばれる通信プロトコルを用いて接続されるものである．NMEA0183 規格（IEC61162-1 ，IEC61162-2）においては 7 ビット ASCII による非同期シリアル通信が，また NMEA2000 規格（IEC 61162-3）においては車載系ネットワークで採用されている CAN（Controller Area Network）方式にもとづく通信が，それぞれ行われる．このネットワーク構成例は，船内ネットワーク構成機器の種別から複数の階層に分けて構成するという点において，図 1 に示された自動操船システムのネットワークモデルと同様の考え方にもとづくものである．しかし，NMEA 規格はいずれも，送受信機器がそれぞれの通信相手の正当性を認証するための仕組みを持たず，また，伝送されるデータは暗号化されることなく送受信されるため，例えば既定のフォーマットに則りかつ誤ったデータフィールドを有するような不正な伝送データがインターネット側や船内に攻撃者が設置した機器から注入される危険性がある．

現在，業界団体においてイーサネットベースの次期 NMEA 規格の策定が行われているところであるが，自動運航船内ネットワークの通信規格として現行 NMEA 規格がそのまま利用されるとするならば，上記で上げたセキュリティ上の脅威にさらされないよう，ネットワーク内に IDS や IPS のような伝送パケット監視・異常パケット検出のための機器を設置することが必要である．自動操船システムは，異常データの混入に起因するシステム障害により船舶の正常運航が行えなくなったとしても，陸上のように有人の対処班を派遣して解決を図ることは容易でないことから，不正なデータを注入された機器の異常動作を迅速に検出し初動処理・回復処理を行うような自己診断機能の実装が必要である．

3. 提案手法

自動運航船に対するサイバー攻撃は，その攻撃による影響が船舶の座礁や衝突等といった人命・船体の安全性を脅かすハザードを引き起こす．このようなハザードを引き起こさないために自動操船システムに求められる機能要件は例えば文献[16][17]に示されており，他船と衝突することなく予定航路を計画するための自動避航機能や計画航路に追従して運航するための自動操舵機能が挙げられる．もしサ

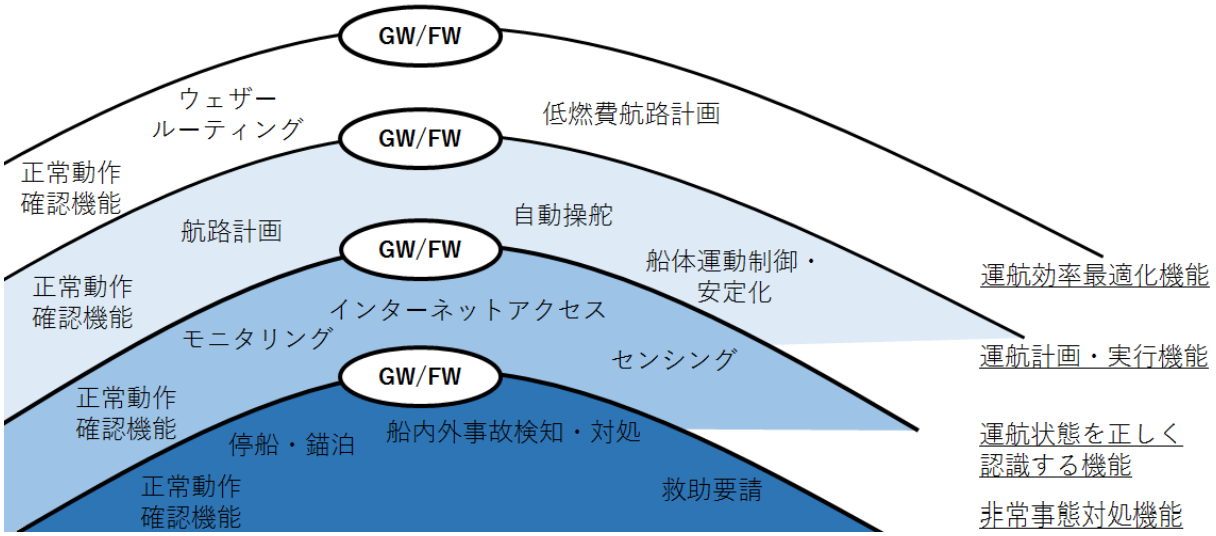

図 3 自律機能の重要度にもとづくゾーニング

イバー攻撃によりこれらの機能が正常に動作しなくなれば，人命や船体の損傷等の深刻な事故が発生する可能性があるという点で，安全な自動運航プロセスを実現するために自動操船システムに求められる自律機能そのものが攻撃者から保護すべき重要な情報資産である．提案手法では，自動操船システムが有するべき自律機能に関して，その正常機能が失われた際に発生する可能性のあるハザードの深刻度や運航継続に及ぼす影響の大きさにしたがって，自律機能の重要度を定めゾーニングを行う．より重要度の高い自律機能を構成する搭載機器やプログラムがサイバー攻撃によって不正動作や不稼動状態に陥らないように優先的にソフトウェアあるいはハードウェア上の保護措置を施すことができるよう，セキュアな自動操船システムアーキテクチャを示す．図 3 に機能維持の重要度にもとづいてゾーニングした自律機能マップを示す．

3.1 非常事態対処に関する自律機能

自動操船システムに求められる自律機能のうち，人命傷害や沈没等のハザードを防止，検出，対処するための機能は，サイバー攻撃から保護すべき自律機能として最も重要なものである．本機能は，自動運航船が海難事故や火災に直面した場合に必要になる機能と位置づけられる．本機能には以下の機能が含まれる．

- 船内外災害検知・対処機能
- 救助要請機能
- 停泊・錨泊機能

船内事故検知・対処機能は，船内で発生した火災や浸水を迅速に検出するとともに消化，排水等の防災措置を施すために重要である．災害検知を行う機器として，煙/熱感知器，浸水検知センサが挙げられる．災害の検出を船内ネットワーク内に通知する機器として BNWAS（航海当直警報装置）や火災報知器，浸水警報装置が挙げられる．災害に対処するための機器として，消火装置や排水処理装置が挙げられる．

救助要請機能は，自船が海難事故に遭遇し救助を必要としている状況であることを示す遭難信号を発出するための機能であり，捜索救助用レーダトランスポンダや EPIRB（非常位置指示無線標識），双方向無線電話等，GMDSS（「海上における遭難及び安全に関する世界的制度」）で規定された無線等通信機器により構成される．

錨泊・停泊機能は，海難時や遭難時に船舶の運航プロセスを中止し，洋上に停泊するための機能である．特に DPS（自動船位保持装置）による船位保持機能が正常であることにより，運航継続できない状況において漂流することなく洋上で救助を待つことが可能となる．

3.2 運航状態を正しく認識するための自律機能

運航状態を正しく認識するための自律機能が正常に動作しない場合，少なくとも非常事態対処に関する自律機能が作動すれば火災や沈没等のハザードを防ぐことができるものの，他船や浮標物との衝突，座礁等を誘発することでより深刻な事態に陥る可能性があるとともに，現在の運航状態が異常であるか否かを判断することができない．したがって，非常事態対処機能に次いで自船の運航状態を正しく認識するための自律機能の保護が重要である．本機能には以下の機能が含まれる．

- インターネットアクセス機能
- 自船状態・環境センシング機能
- 運航状態モニタリング機能

衛星回線を経由したインターネットアクセス機能は，特に GPS による位置情報及び時刻情報を取得するために重要である．なおインターネットアクセス機能は本自律機能以外の自律機能が作動する上でも情報ダウンロードや陸上管理センターによる遠隔制御を行うために必要となる重要

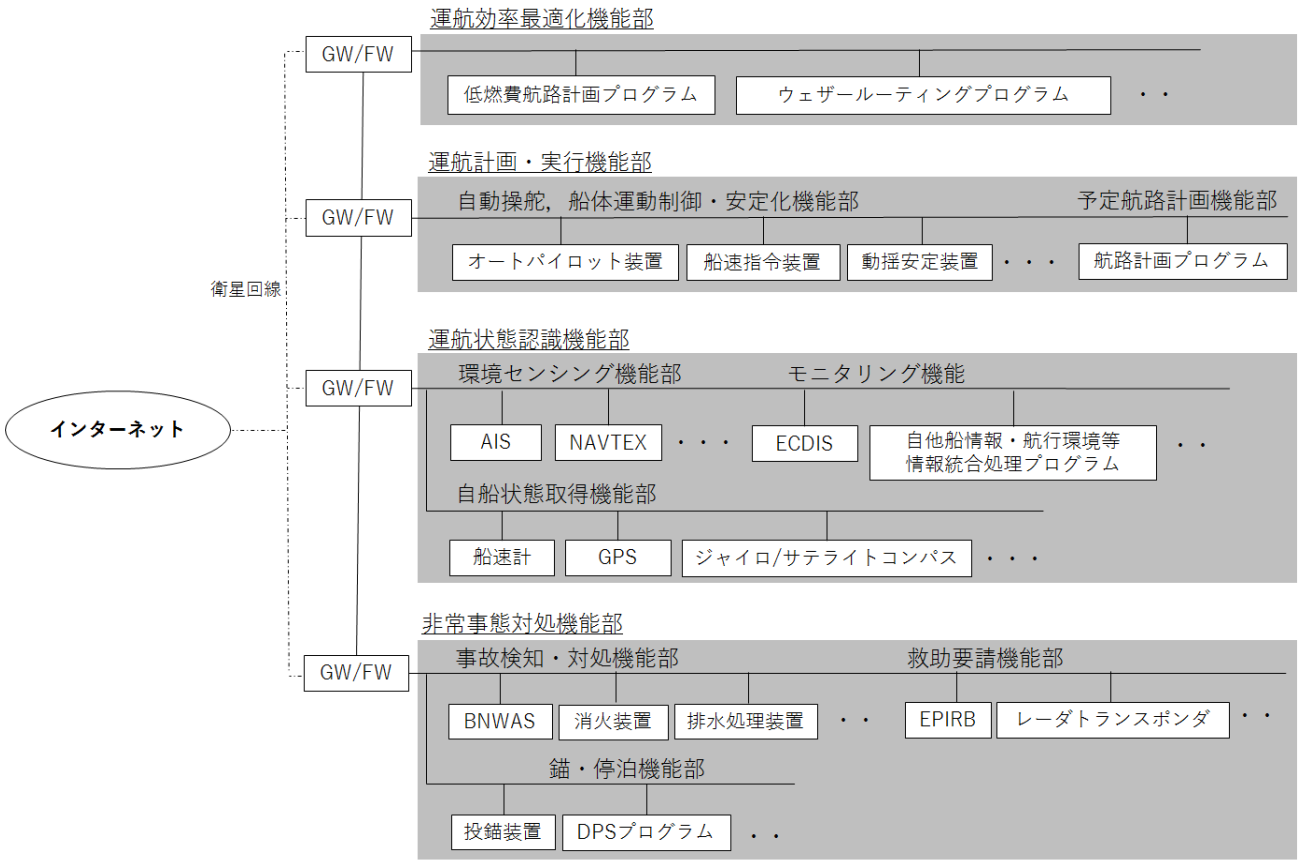

図 4　自律機能の重要度にもとづく自動操船システムアーキテクチャ

な機能である．

自船状態を計測する機器として，船速計，GPS，ジャイロコンパス/サテライトコンパス，風向風速センサが挙げられる．環境センシングは，レーダや AIS, NAVTEX, LiDAR, ソナー等によって行われる．運航状態モニタリング機能は，センシング・取得された自他船情報に加えて，ECDIS（電子海図表示装置）によって提供される地理データを複合することにより実現される．

3.3　運航計画・実行に関する自律機能

運航計画・実行に関する自律機能が正常に動作しない場合，少なくとも運航状態が正しく認識されていれば，運航計画・実行上の不備により運航プロセスが失敗する可能性があることが判断できる．したがって，運航状態を正しく認識するための自律機能に次いで，運航計画・実行に関する自律機能の保護が重要である．本機能には以下の機能が含まれる．

- 予定航路計画機能
- 自動操舵機能
- 船体運動制御・安定化機能

予定航路計画機能は，運航状態を正しく認識するための自律機能を構成する計測器・センサ類から取得・センシングされた情報や電子海図データあるいはインターネットから取得した航行環境情報・航行警報等にもとづき自船の予定航路を計画する機能である．

自動操舵機能及び船体運動制御・安定化機能は，予定航路計画機能によって計画された航路上を逸脱することなく追従するための機能であり，オートパイロット/スラスタ装置，船速指令装置，動揺安定装置等により実現される．

3.4　運航効率最適化に関する自律機能

本機能は，目的港までの低燃費航路や悪天候回避航路などの大域的に最適化された航路を計画するためのものである．本機能には以下の機能が含まれる．

- ウェザールーティング機能
- 低燃費航路計画機能

ウェザールーティング機能は，大域的な気象海象情報を利用して悪天候等を避けた予定航路を計画するための機能である．輻輳海域を避けた大域航路計画機能も必要となる．本自律機能を構成するソフトウェア・プログラムに異常動作や障害が発生した場合には，運航プロセスの継続に危機的なハザードは発生しないものの，航海日程の遅延やコスト増加といった，効率的な運航を阻害する問題が発生する．

3.5　正常動作を確認するための自律機能

非常事態対処，運航状態認識，運航計画・実行機能及び

運航効率最適化のそれぞれに関する自律機能には，自らの自律機能を構成する機器やプログラムに異常動作が発生していないかを確認・判断するための機能が必要である．このような機能によって機器やプログラムの異常が検出された場合には，それらの異常動作によってより重要な自律機能にも異常動作が伝播しないよう，GW や FW により不正トラフィックを遮断する機能が必要である．

3.6 自動操船システムのためのゾーニングモデル

自動操船システムに求められる自律機能を，(1)非常事態対処機能，(2)運航状態認識機能，(3)運航計画・実行機能，(4)運航効率最適化機能の優先順位で，サイバー攻撃に起因した不正動作や障害から優先して保護すべき機能であると位置づける．各自律機能を構成する機器，プログラムを階層的にネットワーク化するとともに，各自律機能を構成する層間は GW あるいは FW を配置する．インターネットあるいは船内侵入した攻撃者による不正指令・データの注入等は，それらの指令・データが送られた機器あるいはプログラムが配置されたネットワーク層の入口となる GW/FW によって悪性検査の判定処理とともに遮断することができるよう構成する．

3.7 自動操船システムアーキテクチャ

自律機能の重要度にもとづくゾーニングモデルを利用した自動操船システムアーキテクチャを図 4 に示す．自動操船システムが備えるべき自律機能である，非常事態対処機能，運航状態認識機能，運航計画・実行機能，運航効率最適化機能のそれぞれについて，同機能を構成するための機器及びプログラムを階層化し配置する．ここで，衛星回線によるインターネットアクセス機能は，運航状態認識機能部のみならず他の階層の自律機能が動作する上でも必要となる場合がある．そのためインターネットから船内ネットワークへ送られる指令やデータは，それらの指令やデータが渡される自律機能部の入口側に設置された GW/FW によって別個に悪性検査が行われる構成とする．

4. おわりに

本稿では，自動操船システムに求められる機能要求・安全要求を分析しサイバーセキュリティ上の脅威にさらされても安全かつセキュアな運航プロセスを継続するための自動操船システムアーキテクチャを提案した．提案するアーキテクチャは，自動操船システムに求められる自律機能を，その機能の不正な中断等による影響の性質や重要度によって大別するとともに，階層的にネットワーク化することでゾーニングを行うものである．特に非常事態対処に関する自律機能及び運航状態を正しく認識するための自律機能はそれ自体が重要な情報資産であり，これらの機能を構成する機器やプログラムは SW と HW の両面から強固な保護が必要である．

参考文献

[1] Ø. J. Rødseth, H. C. Burmeister, “Developments Towards the Unmanned Ship,” in Proc. of the 9th Intl. Symposium ISIS(INFORMATION ON SHIPS), August 30-31, Germany, 2012.

[2] H. C. Burmeister, Ø. J. Rødseth, “Beyond the e-Navigation implementation plan: Development towards the unmanned merchant vessel?,” in Proc. of the e-Navigation conference on the ferry M/S Pearl Seaways, January 28-30, 2014.

[3] Ø. J. Rødseth, H. C. Burmeister, and T. Porathe, “Maritime Unmanned Navigation through Intelligence in Networks THE MUNIN Project,” in Proc. 12th Intl. Conf. on Computer and IT Applications in the Maritime Industries(COMOPIT), Italy,2013.

[4] L. Kretschmann, Ø. J. Rødseth, B. S. Fuller, H. Noble, J. Horahan, and H. McDowell, “MUNIN D9.3: Quantitave assessment,” 2015, http://www.unmanned-ship.org/munin/wp-content/uploads/2015/10/MUNIN-D9-3-Quantitative-assessment-CML-final.pdf (accessed August. 20, 2019).

[5] Ø. J. Rødseth, A. Tjora, “A system architecture for an unmanned ship,” in Proc. 13th Intl. Conf. on Computer and IT Applications in the Maritime Industries(COMPIT), UK, 2014, 2014.

[6] Ø. J. Rødseth et al., “Communication architecture for an unmanned merchant ship,” in Proc. MTS/IEEE OCEANS 2013.

[7] Ø. J. Rødseth, H. C. Burmeister, “Risk Assessment for an Unmanned Merchant Ship,” the International Journal on Marine Navigation and Safety of Sea Transportation(TRANSNAV), vol. 9, no. 3, pp. 357-364, 2015.

[8] K. Wróbel, P. Krata, J. Montewka, and T. Hinz, “Towards the Development of a Risk Model for Unmanned Vessels Design and Operations,” the International Journal on Marine Navigation and Safety of Sea Transportation(TRANSNAV), vol. 10, no. 2, pp. 267-274, 2016.

[9] T. Humphreys, “Secure PNT for Autonomous Systems,” Stanford PNT Challenges and Opportunities Symposium, Nov. 14, 2013.

[10] J. Bhatti, T. Humphreys, “Hostile control of ships via false GPS signals: Demonstration and detection,” the journal of the Institute of Navigation, 2016.

[11] M. Balduzzi, A. Pasta, and K. Wilhoit, “A security evaluation of AIS automated identification system,” in Proc. the 30th Annual Computer Security Applications Conference (ACSAC '14), pp. 436-445, Dec 8-12, 2014, USA.

[12] J. Petit, B. Stottelaar, M. Feiri, and F. Kargl, “Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and LiDAR,” Black Hat Europe 2015.

[13] 松本勉, “計測セキュリティとは何か,” 計測セキュリティフォーラム 2018.

[14] T. Kimberly, J. Kevin, “Cyber-Risk Assessment for Autonomous Ships,” in Proc. Intl. Conf. on Cyber Security and Protection of Digital Services(Cyber Security), June 11-12, UK, 2018.

[15] S. Krile, D. Kezić, and F. Dimc,“NMEA Communication Standard for Shipboard Data Architecture,” Our Sea,International Journal of Maritime Science&Technology,vol. 60, no. 3 pp. 68-81, 2013..

[16] Bureau Veritas, "Guidelines for Autonomous Shipping", *Guidance Note NI 641 DT R00 E*, December 2017.

[17] W. Bruhn, H. C. Burmeister, L. Walther, J. Moæus, M. Long, M. Schaub, and E. Fentzahn, “MUNIN D5.2: Process Map for Autonomous Navigation,” 2015, http://www.unmanned-ship.org/munin/wp-content/uploads/2014/01/MUNIN-D5-2-Process-Map-for-Autonomous-Navigation-CML-final.pdf (accessed August. 20, 2019).