【研究活動紹介】

自動運転システム安全設計

-第３報：自動運転システムにおける機能安全コンセプトの事例検討-

Safety Design for Automated Driving Systems

-Third Report: A Case Study of Functional Safety Concepts in Automated Driving Systems-

金子　貴信 *1　　中村　英夫 *1　　深澤　竜三 *1

Takanobu KANEKO　　Hideo NAKAMURA　　Ryuzou FUKASAWA

1. はじめに

自動運転システムには，自動化のレベル [1]に応じて，運転支援のような高速道路での定速走行・車間距離制御（ACC），車線逸脱防止システム（LKAS）などを組み合わせた運転支援から自動運転・無人運転までが含まれる．これらのシステム開発や実用化に向けての法規制などの検討が世界各国で進められている．一方で，自動運転システムを構成する電気/電子システム（以下，E/E システムと略す）に故障が発生し，走行中に前方障害物に衝突するなどの事故（危害）によるリスクを低減するための安全設計が必要と考えられ，自動車用 E/E システムの機能安全規格 ISO 26262[2]（2011 年 11 月発行）の適用が考えられる．この規格は，E/E システムに故障が発生した際にフェールセーフ（機能停止）やフェールオペレーショナル 注 1)（機能継続）などの安全機構を設けることにより，ドライバ，乗員や交通参加者等への危害となるハザード（危険）を許容可能なレベルに低減する考え方である．本検討では，周辺監視義務を含む運転主権がシステム側にある自動化レベル 3 以上を想定した自動運転システムの機能レベルアーキテクチャ [3]をベースとして，ISO 26262 Part3 のプロセスに従った機能安全コンセプトを策定し，産業界で利活用するための 1 つの事例を作成した．また，今後の課題についての検討結果も報告する．

なお，本報告は一般財団法人日本自動車研究所が受託した経済産業省の委託事業「平成 27 年度次世代自動運転システム研究開発・実証プロジェクト」の「自動走行システム安全設計」に関わる部分を紹介するものである．

2. 自動運転システムのアーキテクチャ

Fig. 1（p2 参照）に自動運転システム（高速道路用）のアーキテクチャ [3]を示す．各種センシング機能で検出された結果などから，ローカルダイナミック MAP が作成される．その情報を基に，目標軌跡，目標車速から操舵角や制駆動力指令値が演算され，操舵，エンジン，ブレーキ系システムに入力される．また，機能安全コンセプトの策定は Fig. 2 に示す ISO 26262 コンセプトフェーズのプロセスに従って実施した．3-5 アイテム定義では ISO 26262 が適用されるシステムの範囲を定義した．次に，3-7 ハザード分析及びリスクアセスメントでは上記アイテムの危険事象を識別，分類し，不合理なリスクを回避するための ASIL 及び安全目標を決定した．3-8 機能安全コンセプトでは機能安全要求を導出し，それらをアーキテクチャに配置した．

Fig. 2　ISO 26262 コンセプトフェーズのプロセス [2]

＊1　一般財団法人日本自動車研究所　ITS研究部

注 1　フェールオペレーショナル：故障が発生してもシステムの動作を継続する．

3. アイテム定義

3 章では Fig. 1 の自動運転システムのアーキテクチャに電源機能を追加し，アイテムとして定義した. Fig. 3 に対象となるアイテムを示す. また，Table 1 にアイテムの IF の各機能について示す. アイテムは Table 1 に記載される IF1-1～IF5-1 により構成される．本検討では自動運転システムのアーキテクチャ内の領域 1（Fig. 1 上段の自律走行に必要となる基本機能）部分に限定してアイテム境界を設定した．なお，IF は Intended Functionality（意図した機能）の略である.

Table 1　アイテムの機能

機能分類	機能No.	機能名
検知	IF1−1	ドライバ入力検知
	IF1−2	NAVI入力検知の故障
	IF1−3	走行周辺環境検出
	IF1−4	GNSS
	IF1−5	車両状態検出
認知	IF2−1	走行周辺環境物体認識
	IF2−2	自車位置推定
	IF2−3	ローカルダイナミックMAP作成
判断	IF3−1	目標軌跡目標車速計画
操作	IF4−1	軌跡追従制御
	IF4−2	操舵角制御
	IF4−3	操舵駆動
	IF4−4	車速制御
	IF4−5	エンジントルク制御
	IF4−6	（車速制御）分配
	IF4−7	スロットル駆動
	IF4−8	ブレーキ力制御
	IF4−9	ブレーキ駆動
	IF4−17	（操舵角制御）切替
	IF4−18	（車速制御）切替
共通	IF5−1	電源機能

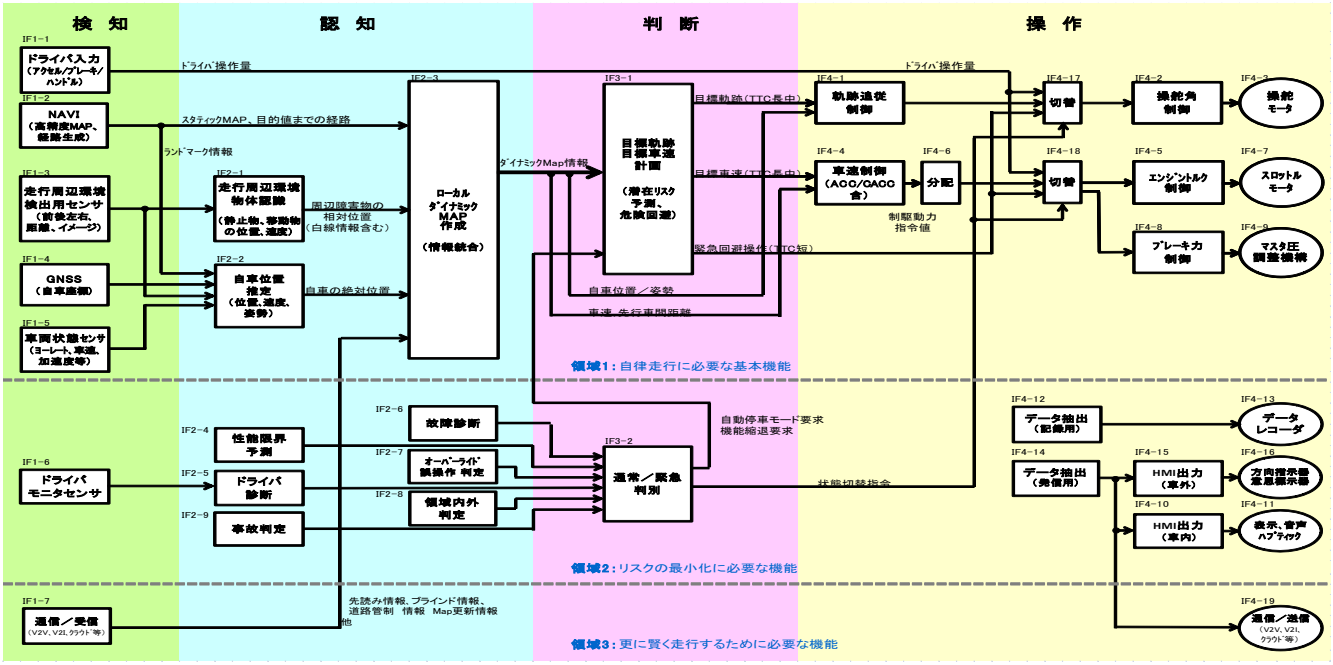


Fig. 1　自動運転システムのアーキテクチャ例[3)]

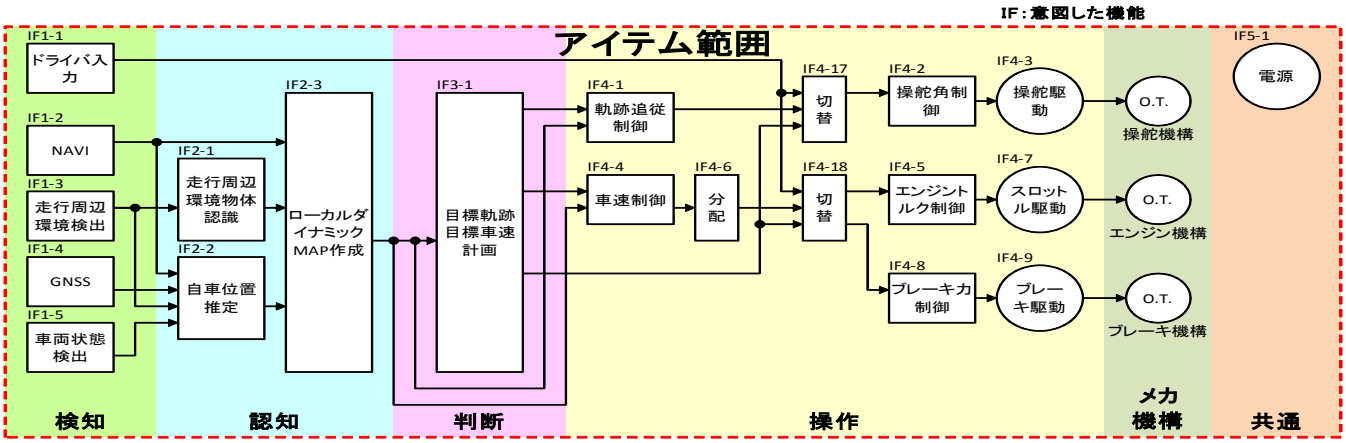


Fig. 3　アイテム範囲

4. ハザード分析及びリスクアセスメント

4 章ではハザード分析を行い，そのハザード（危害の潜在的な源）に関するリスクアセスメントから自動車安全度水準（以下，ASIL と略す）を決定した．

4.1 ハザード分析

ハザード分析ではアイテム定義をもとに，ハザードを抽出した．具体的にはアイテムの各機能が故障したとき，安全機構がない前提で車両ハザードを抽出した．ハザードの発生するシチュエーションは自動運転システムの機能レベルアーキテクチャの策定 [3]で検討した高速道路のユースケース，例えば，ETC 通過，合流，本線走行，カーブなどを想定した．Table 2 に HAZOP[注 2)]よるハザード抽出結果例を示す．

Table 2　ハザードの抽出結果例（×：ハザード抽出）

機能分類	機能 No.	機能故障	車両のハザード					
			HZ1：自動運転において必要な操舵をしない（操舵失陥）	HZ2：自動運転において不必要な操舵をする（セルフステア）	HZ3：自動運転において必要な加速をしない（加速不良）	HZ4：自動運転において不必要な加速をする（急加速）	HZ5：自動運転において不必要な減速をする（急減速）	HZ6：自動運転において必要な減速をしない（制動失陥）
検知	IF1-1	ドライバ入力検知機能の故障	×	×	×	×	×	×
	IF1-2	NAVI入力検知機能の故障						
	IF1-3	走行周辺環境検出機能の故障	×	×	×	×	×	×
	IF1-4	GNSS入力検知機能の故障						
	IF1-5	車両状態検出機能の故障	×	×	×	×	×	×
認知	IF2-1	走行周辺環境物体認識機能故障	×	×	×	×	×	×
	IF2-2	自車位置推定機能の故障	×	×	×	×	×	×
	IF2-3	ローカルダイナミックMAP機能故障	×	×	×	×	×	×
判断	IF3-1	目標軌跡目標車速計画機能故障	×	×	×	×	×	×
操作	IF4-1	軌跡追従制御機能の故障	×	×				
	IF4-2	操舵角制御機能の故障	×	×				
	IF4-3	操舵駆動機能の故障	×	×				
	IF4-4	車速制御機能の故障			×	×	×	
	IF4-5	エンジントルク制御機能の故障			×	×	×	
	IF4-6	（車速制御）分配機能の故障			×	×	×	
	IF4-7	スロットル駆動機能の故障			×	×	×	
	IF4-8	ブレーキ制御機能の故障					×	×
	IF4-9	ブレーキ駆動機能の故障					×	×
	IF4-17	（操舵角制御）切替機能の故障	×	×				
	IF4-18	（車速制御）切替機能の故障			×	×	×	×
共通	IF5-1	電源機能の故障	×		×			×

アイテムの各機能が故障した場合，主なハザードとして操作系（操舵，エンジン，ブレーキ）に着目すると「6 つのハザード（HZ1～HZ6）が抽出」され，上位機能（検知，認知，判断）の故障により，「全てのハザードを生じる可能性」があることがわかった．ただし，以下の上位機能については故障が発生しても直ちにハザードを生じないため分けて考えた．（5.2 節参照）

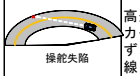
・IF1-2: NAVI による高精度 MAP および経路生成情報は，認知機能に必要分蓄積されている．
・IF1-4: GNSS による自車位置情報が失われても，他の検知機能の情報で暫く補間できる．

なお，ハザードの抽出にあたり，現行の ISO 26262 に従い E/E システムの機能故障を対象とし，例えばセンサの性能限界等については考慮していない．

4.2 リスクアセスメント

4.1 節の各ハザードについてリスクアセスメント（E:曝露，C:コントローラビリティ，S:シビアリティ，の評価）を行った検討例を Table 3 に示す．

Table 3　リスクアセスメントの検討例

No.	区分	アイテム	ハザード	危険事象 イメージ	危険事象
HZ1	操舵失陥	操舵制御	自動運転において必要な操舵をしない		高速道路を自動走行中にカーブで必要な操舵がされず、カーブを曲がれずに車線を逸脱しガードレールと衝突する．
HZ2	セルフステア	操舵制御	自動運転において不必要な操舵をする		高速道路を自動走行で直進している状況で、操舵され，側方の壁に衝突する．
HZ3	加速不良	エンジン制御	自動運転において必要な加速をしない		自動走行している自車が高速道路合流路を走行しており，合流路で加速せずに本線へ合流する．本線を走行している後続車が減速したが自車に衝突する．
HZ4	急加速	エンジン制御	自動運転において不必要な加速をする		高速道路を自車が先行車に高速で追従して自動走行している状況において，加速し続ける．
HZ5	急減速	ブレーキ制御	自動運転において不必要な減速をする		高速道路で後続車が追従走行しているときに自動走行している自車が急減速し，後続車の減速が間に合わず自車に衝突する．
HZ6	制動失陥	ブレーキ制御	自動運転において必要な減速をしない		高速道路の前方のETCレーンで減速している先行車両に自車は追従して自動走行している状況で，減速せず先行車に衝突する．

高速道路を走行している一般的な前提条件（例，

注 2　HAZOP（Hazard and operability study）：ISO26262 でアイテムのハザードを抽出するための手法の 1 つ

車速 100 km/h 走行などの E4 クラスとなる高いシチュエーション）において，各ハザードの最高 ASIL は暫定的に C～D となった．

ここで，コントローラビリティについて自動運転車（レベル 3 以上）のドライバは通常ステアリングから手を離しており，セカンドタスクを行っている状態や覚醒状態が低下している可能性もあるため，衝突に至る前にドライバの回避行動が間に合わないと考え，C3 クラス（90%未満のドライバが回避）と仮定している．なお，Table 3 のハザード HZ3，HZ5 については，後続車のドライバ反応時間からコントローラビリティを評価した．

5. 安全目標および安全方策の策定

5 章では，ASIL を伴う各危険事象（ハザーダスイベント）に，安全目標，安全状態を定めて，安全目標侵害に繋がる機能故障モードを安全分析（FMEA などの手法）を行うことにより識別し，安全方策（追加機能）を検討した．

5. 1 安全目標と安全状態の決定

ハザード分析及びリスクアセスメントの結果から安全目標（SG），安全状態（SS）を決定した．Table 4 に結果を示す．安全目標は 4 章で抽出した急加速，急減速，操舵失陥などの「各ハザードを防止すること」とし，暫定的に ASIL C～D を付与した．また，安全状態への考え方は「高速道路走行中に自動運転システムに故障が発生した場合，ドライバに引き継ぐ．または，ドライバが所定時間内に引き継がない場合，路側帯等の安全な場所に停車してドライバに引き継ぐ．」とし，「ドライバに引き継ぐまで，自動運転システムの制御を継続する．」を実現するため，安全状態は，「各制御系の機能を継続する．」とした．

Table 4 安全目標（SG），安全状態（SS）例

安全目標（SG）		安全状態（SS）
SG No.	内容	
SG1	高速道路での自動運転おいて危険事象に至る操舵失陥を防止する	操舵系の機能を継続する
SG2	高速道路での自動運転おいて危険事象に至る不必要な操舵を防止する	操舵系の機能を継続する
SG3	高速道路での自動運転おいて危険事象に至る加速不良を防止する	スロットル制御系の機能を継続する
SG4	高速道路での自動運転おいて危険事象に至る急加速を防止する	スロットル制御系の機能を継続する
SG5	高速道路での自動運転おいて危険事象に至る急減速を防止する	ブレーキ制御系の機能を継続する
SG6	高速道路での自動運転おいて危険事象に至る制動失陥を防止する	ブレーキ制御系の機能を継続する

5. 2 安全方策の検討

検討対象とした自動運転システムについて，5.1 節の安全目標の侵害に繋がる機能故障モードを識別し，それらへの安全方策を検討した．

Table 5 に機能故障に関する安全方策の例（抜粋）を示す．安全方策を検討した結果，「主系の故障を検出した場合，主系を停止し，冗長系で継続する」方策（SM1～SM5）が得られた．なお，本節で記載している冗長系とは二重系以上を意図している．また，ドライバに故障の発生と運転の引継ぎを告知するため，ドライバへの警告機能を設ける方策（SM6）が得られた．

Table 5 では省略しているが，NAVI 入力検知機能の故障と GNSS 入力検知機能の故障については，自動運転中に故障が生じても直ちに安全目標を侵害する可能性が低いと想定されるので，安全機構としては故障検出機能のみ設定し，冗長系機能は設けなかった．

Table 5 安全方策例（抜粋）

SM	機能故障	安全方策
SM 1–3	走行周辺環境検出機能の故障	走行周辺環境検出機能の故障を検出する機能を設け，故障を検出した場合，走行周辺環境検出機能の出力を停止し，冗長系走行周辺環境検出機能に切り替えて，安全状態に遷移するまで検知を継続する．
SM 2–1	走行周辺環境物体認識機能の故障	走行周辺環境物体認識機能の故障を検出する機能を設け，故障を検出した場合，走行周辺環境物体認識機能の出力を停止し，冗長系走行周辺環境物体認識機能に切り替えて，安全状態に遷移するまで認知を継続する．
SM 3–1	目標軌跡目標車速計画機能の故障	目標軌跡目標車速計画機能の故障を検出する機能を設け，故障を検出した場合，目標軌跡目標車速計画機能の出力を停止し，冗長系目標軌跡目標車速計画機能に切り替えて，安全状態に遷移するまで判断を継続する．
SM 4–1	軌跡追従制御機能の故障	軌跡追従制御機能の故障を検出する機能を設け，故障を検出した場合，軌跡追従制御機能の出力を停止し，冗長系軌跡追従制御機能に切り替えて，安全状態に遷移するまで制御を継続する．
SM 4–2	操舵角制御機能の故障	操舵角制御機能の故障を検出する機能を設け，故障を検出した場合，操舵角制御機能の出力を停止し，冗長系操舵角制御機能に切り替えて，安全状態に遷移するまで制御を継続する．
SM 4–4	車速制御機能の故障	車速制御機能の故障を検出する機能を設け，故障を検出した場合，車速制御機能の出力を停止し，冗長系車速制御機能に切り替えて，安全状態に遷移するまで制御を継続する．
SM 4–5	エンジントルク制御機能の故障	エンジントルク制御機能の故障を検出する機能を設け，故障を検出した場合，エンジントルク制御機能の出力を停止し，冗長系エンジントルク制御機能に切り替えて，安全状態に遷移するまで制御を継続する．
SM 4–8	ブレーキカ制御機能の故障	ブレーキカ制御機能の故障を検出する機能を設け，故障を検出した場合，ブレーキカ制御機能の出力を停止し，冗長系ブレーキカ制御機能に切り替えて，安全状態に遷移するまで制御を継続する．
SM 5–1	電源機能の故障	電源機能の故障を検出する機能を設け，故障を検出した場合，電源機能の出力を停止し，冗長系電源機能に切り替えて，安全状態に遷移するまで電源供給を継続する．
SM 6–1	上記機能の故障	警告機能を設け，主機能に故障が検出された場合，ドライバへ通知する．

6. 機能安全コンセプトの策定

6 章では「機能安全コンセプト」を策定し，安全アーキテクチャ（冗長構成，代替構成など）の検討を行った．

6.1 機能安全コンセプト

5 章で各機能の故障について安全方策を導出した．今回の安全方策，「主系の故障を検出した場合，主系を停止し，冗長系で継続する」を適用すると，検知，認知，判断系および操作系の各系において，各機能ブロックは，基本的に Fig. 4 に示すような冗長構成になる．

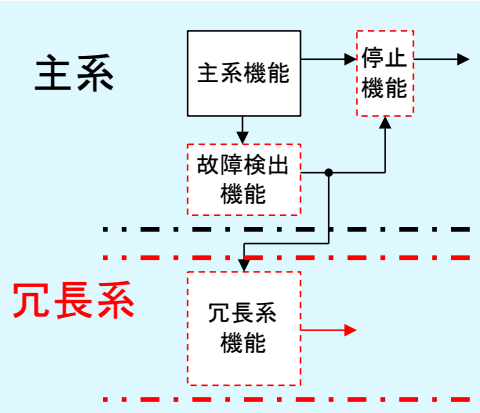


Fig.4 安全方策の基本ブロック構成

Table 5 の安全方策を参照し，Fig. 4 に示す機能ブロック（破線）を要求として記述すると，Table 6 に示す機能安全要求が導出された．（NAVI 入力検知機能および GNSS 入力検知機能などを省略）

次に，アイテム定義での初期アーキテクチャ（Fig. 3）に，Table 6 の機能安全要求を配置して更新すると，Fig. 5（p6 参照）に示すアーキテクチャとなった．上段の主系に対して下段に冗長系が配置されている．これらの Table 6 と Fig. 5 により機能安全コンセプトの 1 つの事例が策定された．

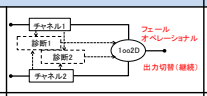
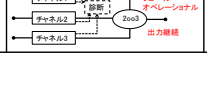
6.2 安全アーキテクチャ

自動運転システムでは，5.1 節の安全目標および安全方策の検討で述べたように，「システムに故障が発生した場合，ドライバに運転を引き継ぐまでシステムの機能を継続する．」とした場合，フェールオペレーショナルな安全アーキテクチャが必要と考えられる．具体的な冗長系の安全アーキテクチャの例を Table 7 に示す．

Table 6 機能安全要求例（抜粋）

機能安全ブロック	機能安全要求
FSR 1.3.1	走行周辺環境検出機能（主系）の故障を検出する機能を設けること．
FSR 1.3.2	走行周辺環境検出機能（主系）の故障を検出した場合，走行周辺環境検出機能（主系）の出力を停止すること．
FSR 1.3.3	冗長系走行周辺環境検出機能を設け，検知を継続すること．
FSR 2.1.1	走行周辺環境物体認識機能（主系）の故障を検出する機能を設けること．
FSR 2.1.2	走行周辺環境物体認識機能（主系）の故障を検出した場合，走行周辺環境物体認識機能（主系）の出力を停止すること．
FSR 2.1.3	冗長系走行周辺環境物体認識機能を設け，認知を継続すること．
FSR 3.1.1	目標軌跡目標車速計画機能（主系）の故障を検出する機能を設けること．
FSR 3.1.2	目標軌跡目標車速計画機能（主系）の故障を検出した場合，目標軌跡目標車速計画機能（主系）の出力を停止すること．
FSR 3.1.3	冗長系目標軌跡目標車速計画機能を設け，判断を継続すること．
FSR 4.1.1	軌跡追従制御機能（主系）の故障を検出する機能を設けること．
FSR 4.1.2	軌跡追従制御機能（主系）の故障を検出した場合，軌跡追従制御機能（主系）の出力を停止すること．
FSR 4.1.3	冗長系軌跡追従制御機能を設け，制御を継続すること．
FSR 4.2.1	操舵角制御機能（主系）の故障を検出する機能を設けること．
FSR 4.2.2	操舵角制御機能（主系）の故障を検出した場合，操舵角制御機能（主系）の出力を停止すること．
FSR 4.2.3	冗長系操舵角制御機能を設け，制御を継続すること．
FSR 4.4.1	車速制御機能（主系）の故障を検出する機能を設けること．
FSR 4.4.2	車速制御機能（主系）の故障を検出した場合，車速制御機能（主系）の出力を停止すること．
FSR 4.4.3	冗長系車速制御機能を設け，制御を継続すること．
FSR 4.5.1	エンジントルク制御機能（主系）の故障を検出する機能を設けること．
FSR 4.5.2	エンジントルク制御機能（主系）の故障を検出した場合，エンジントルク制御機能（主系）の出力を停止すること．
FSR 4.5.3	冗長系エンジントルク制御機能を設け，制御を継続すること．
FSR 4.8.1	ブレーキ力制御機能（主系）の故障を検出する機能を設けること．
FSR 4.8.2	ブレーキ力制御機能（主系）の故障を検出した場合，ブレーキ力制御機能（主系）の出力を停止すること．
FSR 4.8.3	冗長系ブレーキ力制御機能を設け，制御を継続すること．
FSR 5.1.1	電源機能（主系）の故障を検出する機能を設けること．
FSR 5.1.2	電源機能（主系）の故障を検出した場合，電源機能（主系）の出力を停止すること．
FSR 5.1.3	冗長系電源機能を設け，電源供給を継続すること．
FSR 6.1.1	警告機能を設け，故障を検出した場合，ドライバへ通知すること．

Table 7 フェールオペレーショナルの安全アーキテクチャ例（XooY：X out of Y，D=Diagnostics)[4)]

安全アーキテクチャ		1次故障発生時	説明
1oo2D		継続（1oo1D）	1 out of 2 channel architecture with diagnostics 故障診断付きチャネルが2系統、並列にあり、一方のチャネルに故障が発生した場合，出力を停止し，正常側に切り替えて出力は継続される
2oo2D		継続（1oo1D）	2 out of 2 channel architecture with diagnostics 故障診断付きチャネルが2系統、並列にあり、一方のチャネルに故障が発生した場合，出力を停止し，正常側のチャネルで出力は継続される
2oo3		継続（1oo2）	2 out of 3 channel architecture チャネルが3系統、並列にあり、多数決により2系統以上の一致で出力は継続される

本検討では Table 7 の安全アーキテクチャを例としてマルコフモデル 注 3)を作成し，ベースとなる各チャネルの故障率を一定とした条件でチャネル切替機能も含めて定量的な比較検討を行った．その結果，1oo2D，2oo2D，2oo3 の各構成についての信頼度は概ね同等のポテンシャルとなり，いずれも適用可能であることが分かった．

注 3 マルコフモデル：例，故障発生確率を予測するモデル化手法の 1 つ

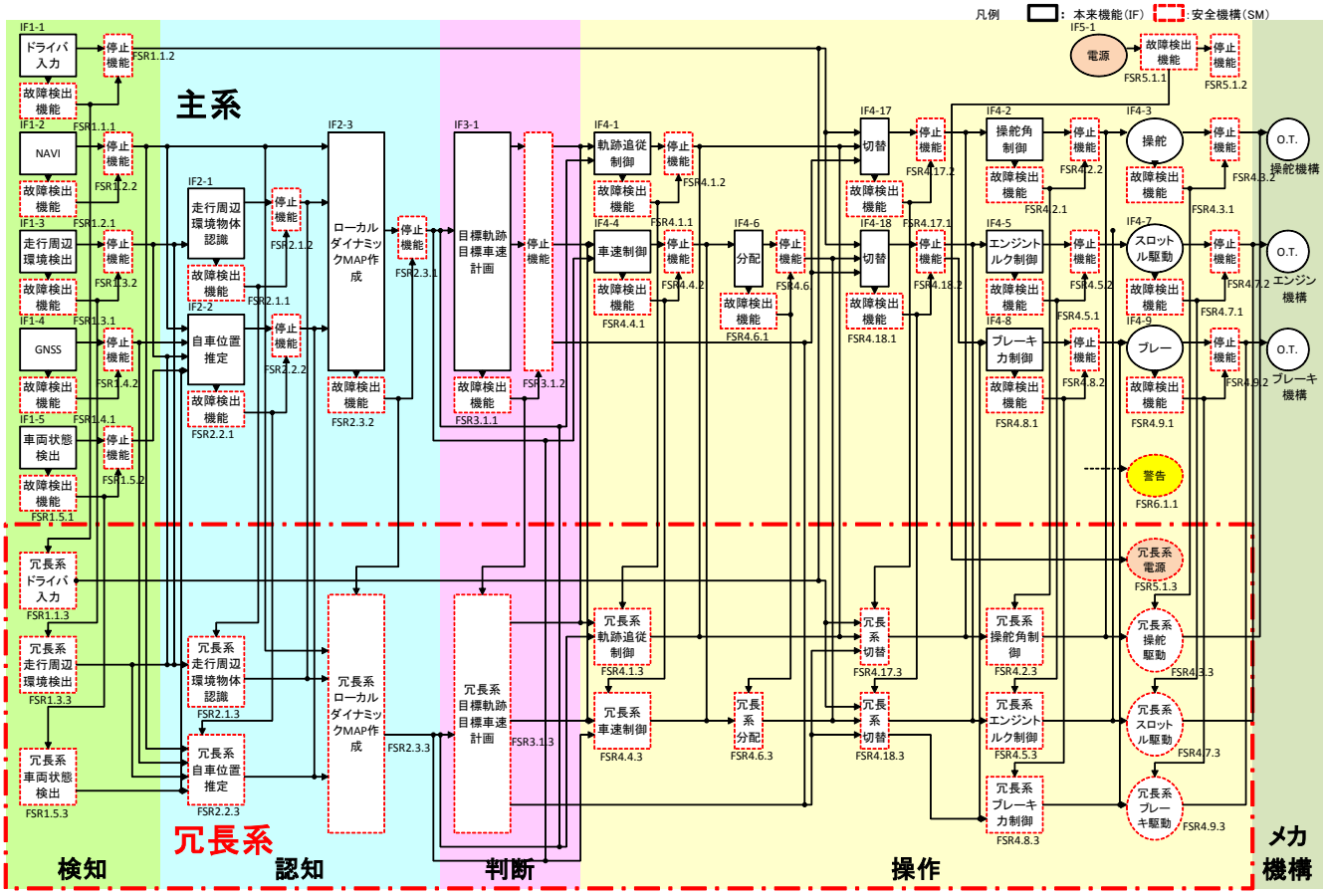


Fig. 5　機能安全要求の配置例

7. まとめと今後の課題

本検討では自動運転システム（レベル 3 以上）の安全設計を行うために現行の機能安全規格に基づき，故障についての機能安全コンセプトを策定した．以下にまとめと課題を整理する．

7. 1　機能安全コンセプトのまとめ

機能安全コンセプトの策定における結果を以下にまとめる．

・自動運転システム（レベル 3 以上，高速道路用）の「走る」，「曲がる」，「止まる」について，6 つのハザードが抽出され，最高 ASIL は暫定的に C～D となった．

・自動運転の E/E システムの機能安全コンセプトで，ドライバに運転を引継ぐまで「機能を継続する」を安全状態とすると，「冗長系（2 重系，3 重系など）」の安全方策が得られた．また，1oo2D, 2oo2D, 2oo3 などの安全アーキテクチャ例が適用可能である．

・アイテム内の各機能（電源を含む）に対して，「故障検出」「機能停止」「冗長系による機能継続」の機能安全要求が導出された．（NAVI, GNSS は「故障検出」「機能停止」のみ）

・警告コンセプトとして，「ドライバへ故障発生および運転の引継ぎを通知する」という安全要求が導出された．

7. 2　今後の課題

自動運転システム（レベル 3 以上，高速道路用）の機能安全コンセプトの策定における今後の課題を以下に整理する．

・故障以外の性能限界，ミスユース（誤操作，誤使用），ドライバ状態など，Fig. 1 基本アーキテクチャ内の第 2 領域（リスクの最小化に必要な機能）を考慮した検討が必要である．

・今回は設定した安全状態に従って各機能を冗長

化する機能安全コンセプトとしたが，各機能の使い方や特性を検討した上で，機能毎の最適化（異種冗長など）や，一部機能（例，エンジン制御）については，縮退などを考慮すると安全状態の見直しも必要と考えられる．また，故障発生後にドライバへ引き継ぐまでを機能継続とすると適切な継続時間の検討も必要である．

・ドライバのコントローラビリティは C3 クラスと仮定して暫定的に ASIL 評価を実施しているが，故障時にドライバへ引継ぎ要求を告知した後のコントローラビリティは被験者評価などを通じて確認し，ASIL を再評価することが必要である．

8. 最後に

自動運転に関する E/E システムの安全性の検討に関する課題は多い．本検討では機能安全規格に従って E/E システムの故障を対象に検討を行い，産業界で共有し，議論できる事例を作成した．しかしながら，自動運転システムの場合，故障以外の性能限界，ドライバの誤操作なども考慮する必要がある. 故障ではないこれらの扱いについては，ISO 26262 2nd Edition に向けた改訂と並行して議論されており，それらの動向を把握しながら，さらなる検討が必要である．

最後に，本プロジェクトに参加された方々のご協力に感謝いたします．

参考文献

1) National Highway Traffic Safety Administration: http://www.nhtsa.gov (2015.4.20), "Preliminary Statement of Policy Concerning Automated Vehicles"
2) ISO 26262, Road vehicles Functional safety (2011)
3) 平成 27 年度次世代自動運転システム研究開発・実証プロジェクト成果報告書，一般財団法人日本自動車研究所，第 3 編 p.Ⅲ1-156 (2015)
4) IEC 61508-6, Functional safety of electrical /electronic/ programmable electronic safety-related systems, Annex B (2010)