NCES

ATK2-SC3-TP を用いた セーフティガイドライン

Ver.1.0.0

2017/03/24

名古屋大学大学院情報科学研究科附属 組込みシステム研究センター

<目次>

1. 概要

1.1　本書の目的

本書は，safety なシステムを構築する際に，どのように TOPPERS/ATK2-SC3-TP(以降，ATK2-SC3-TP)を使用すれば有効かを示すものである．具体的なシステムの例として，AUTOSAR のドキュメント『Safety Use Case Example』に記載されている『FrontLightManegement(以降，FLM)システム』を題材にして進める．

2. FLM システム

本章では，AUTOSAR『Safety Use Case Example』に記載されている『FLM システム』について記載する．

2.1　FLM システム

2.1.1　システムアーキテクチャ

FLM のシステムアーキテクチャを 図 1 に示す．

FLM システムは，Light Switch，Ignition Key，Headlight L/R，Daytime Running Right（以降，DRL），Human Machine Interface（以降，HMI）で実現されている．

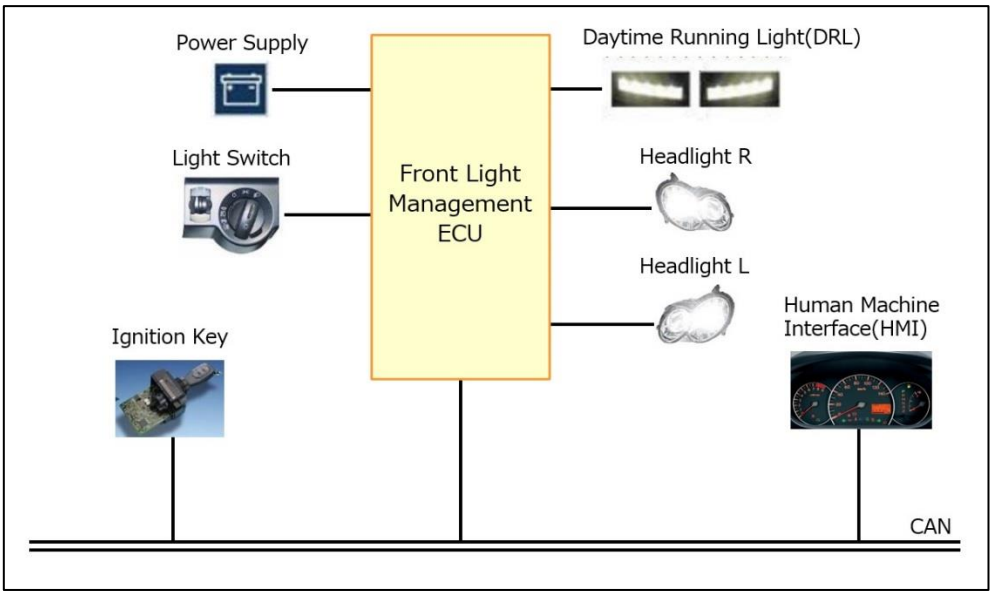

図 1 FLM システムアーキテクチャ

2.1.2　機能

FLM の機能を図 2 に示す．

Light Switch および Ignition Key から Low Beam（以降，LB）のターンオン／ターンオフ状態を検出し，受信したライト要求の解析を行い，LB のアクティブ化／非アクティブ化を行う．LB がアクティブの場合，LB の監視を行い，電球の故障時には HMI に対して，通知を行う．また，両電球が故障した場合には DRL をアクティブ化する．

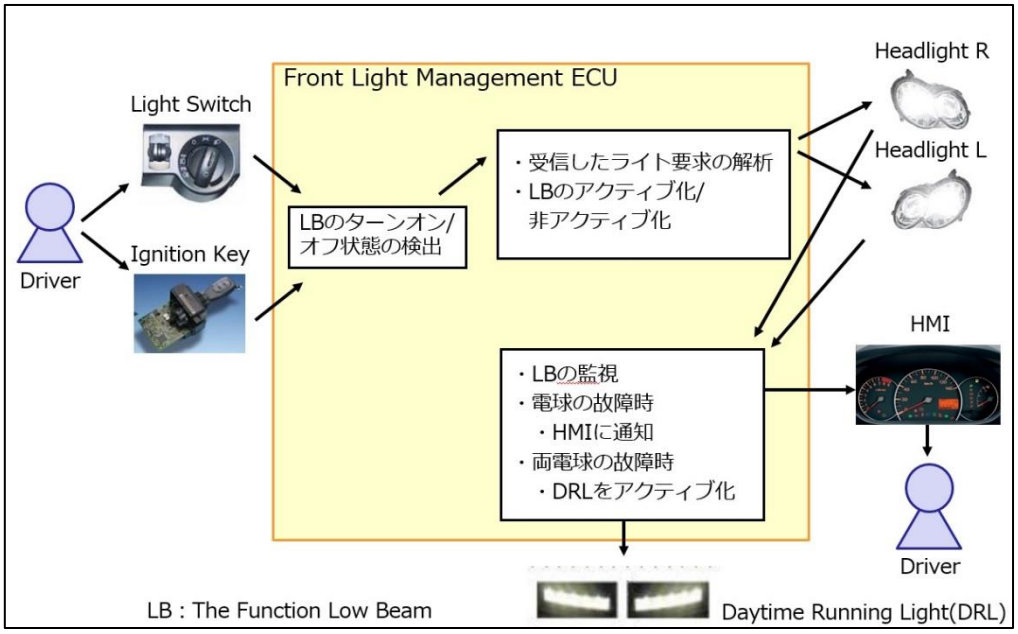

図 2 FLM の機能

2.1.3 Block Diagram

FLM の Block Diagram を図 3 に示す.

FLM システムは 4 つの SWC（SwitchEvent，LightRequest，FrontLightManager，HeadLight）を使用して LB 機能を提供している.

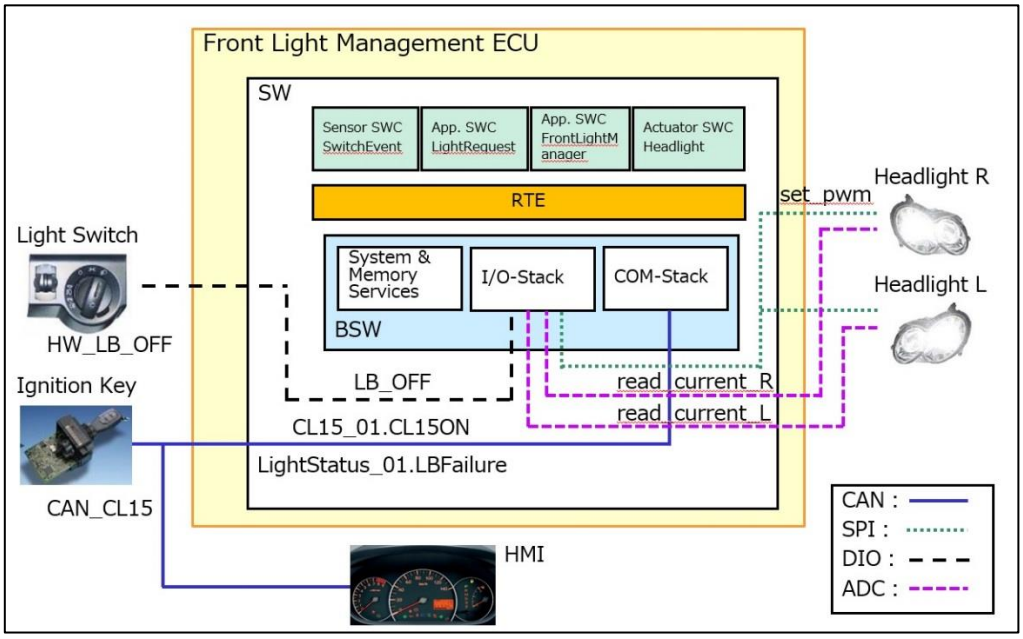

図 3 FLM の Block Diagram

2.2 SWC の機能概要

FLM システムは 4 つの SWC で実現している．本項では各 SWC の機能について説明する．

2.2.1 SwitchEvent SWC

・Light Switch から『LB_OFF』状態を読出し格納
・LightRequest SWC の要求に応じて，『LB_OFF』状態を提供

2.2.2 LightRequest SWC

・SwitchEvent SWC から『LB_OFF』の状態をチェック
・Ignition Key からの CAN Signal『CL15_01』の読出し
・Front Light Manager SWC に対し，ライト点灯／非点灯の要求送信

2.2.3 FrontLightManager SWC

・LightRequest SWC からのライト点灯／非点灯要求の読出し
・Headlight SWC に対し，LB 点灯／非点灯要求を送信
・LB 点灯要求時，Headlight SWC 経由で電球の状態を監視
・電球故障時には，HMI に対し，故障信号『LightStatus_01』を送信
・両電球故障時には，Headlight SWC に対し，DRL の点灯要求を送信
・電球故障時には，Diagnostic Event Manager に故障情報を記録

2.2.4 Headlight SWC

・フロントライトの制御
・電球に電力が供給された場合，電球の電流を監視
・両電球故障時には，DRL の制御

2.3 データの流れ

RTE を介したデータの流れを図 4 に示す.

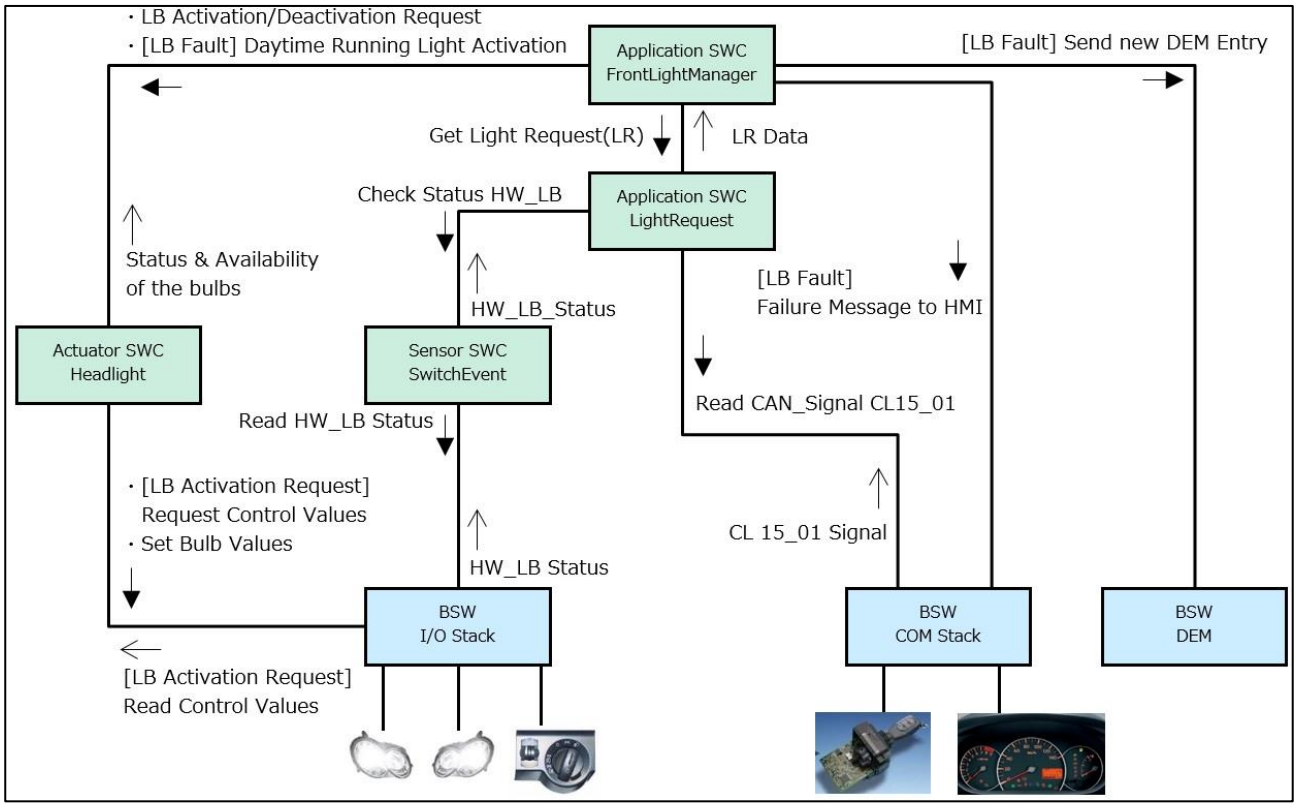

図 4 RTE を介したデータの流れ

2.4 ECU レベルでの安全要求

AUTOSAR『Safety Use Case Example』には FLM ECU レベルでの安全要求が記載されている．安全要求について表 1 に示す.

表 1 FLM ECU レベルでの安全要求

ID	ECU の安全要求	ASIL
ECU01	CAN BUS 『CAN_CL15』の正確な読み出しを保証しなければならない	QM(B)
ECU02	CAN BUS の『CAN_CL15』から論理的な『CL15_01』メッセージへの正確な変換を保証しなければならない	QM(B)
ECU03	AUTOSAR BSW/ RTE を介した『CL15_01』メッセージの正しい配送が保証されなければならない．シグナル『CL15_01.CL15ON』は書き出され、正しくアプリケーション SWC に提供されなければならない	QM(B)
ECU04	ECU は安全目標違反につながる可能性がある，シグナル『CL15ON』に影響を与える潜在的な通信故障を検出しなければならない	B(B)
ECU06	入力『HW_LB_OFF』の正確な読出しを保証しなければならない	QM(B)
ECU07	『HW_LB_OFF』の入力ポートとピンの正確なコンフィギュレーションを保証しなければならない	QM(B)

ECU08	入力『HW_LB_OFF』から論理的なシグナル『LB_OFF』への正確な変換を保証しなければならない	QM(B)
ECU09	AUTOSAR BSW/ RTE を介した『LB_OFF』の正しい配送が保証されなければならない	QM(B)
ECU10	ECU は安全目標違反につながる可能性がある，『LB_OFF』に影響を与える潜在的な故障を検出しなければならない	B(B)
ECU12	アプリケーション SWC は指定された『LB_OFF』と『CL15ON』の状態を判定しなければならない	B
ECU13	アプリケーション SWC は『LB_OFF』，『CL15ON』，指定されたタイミングに基づきライト要求条件を解析しなければならない	B
ECU14	アプリケーション SWC は『LB_OFF』，『CL15ON』の解析結果に基づいて，ライト点灯要求をセットまたはリセットしなければならない. 『CL15_01』メッセージの通信故障が 200ms 以上継続的に検出された場合，および『LB_OFF』の故障が 200ms 以上継続的に検出された場合，ライト点灯要求をセットしなければならない	B
ECU15	両方の電球の故障が継続的に 200ms 検出された場合，アプリケーション SWC は Daytime Running Light を有効にしなければならない	B
ECU16	ライト点灯要求と仕様に従って電球の正確な電源供給は set_pwm コマンド経由で通知される	QM(B)
ECU17	set_pwm 要求からμC SPI 出力への正確な配送を保証しなければならない	QM(B)
ECU18	μC set_pwm 要求からハイサイドドライバへの正確な配送と set_pwm 要求から物理的な出力値『PWM_headlight left』『PWM_headlight right』の正確な変換を保証しなければならない	QM(B)
ECU19	ECU は電球に電力を供給する 2 つの独立したハードウェア経路を提供しなければならない	A(B)
ECU20	電球に電力が供給された場合，Monitoring SWC は電球の状態（read_current_L, read_current_R）を評価しなければならない	A(B)
ECU21	検知された故障は，CAN BUS 『LBFailure』を介して通知されなければならない	A
ECU22	ECU はそれぞれの電球の電流を計測する『HW_current left』，『HW_current right』のために 2 つの独立したチャネルを提供しなければならない	A(B)
ECU23	ECU はフォールトトレラント時間(500ms)に対応して電球の状態測定における経路（μC HW，ECU HW，車両の配線）の故障を検知しなければならない	B
ECU24	AUTOSAR BSW/ RTE を介した電球の電流測定値『read_current_L』，	QM(B)

	『read_current_R』の正確な配送が保証されなければならない	
ECU25	ADC は測定された電流を『read_current_L』，『read_current_R』に変換しなければならない	A(B)
ECU26	SWC 間で正確なデータ交換（タイミングと内容）が保証されなければならない	B
ECU27	送受信間で『CL15_01.CL15ON』の伝送が保証されなければならない	B
ECU28	送受信間で『LightStatus_01.Failure』の伝送が保証されなければならない	A
ECU29	論理『PWM-l-signal』から『SPI BUS message』への正確な変換が保証されなければならない	QM(B)
ECU30	電球に電力が供給された場合，Monitoring SWC は電流を読み出し，電球の状態を提供しなければならない	A(B)

3. FLM システムの再設計

3.1　概要

ATK2-SC3-TP の有効な使用方法を研究するため，FLM システムがパーティショニングされていることを期待していた．しかし，FLM システムでは全ての SWC が ASIL B のため，パーティショニングの必要がなかった．そこで，FLM システムを再設計し，Headlight SWC を ASIL A にすることによってパーティショニングが必要なシステムを構築した．そして，Freedom From interference（以降，FFI）であることを保証するという安全要求を追加し，それに対して分析を行うこととした．

3.2　各 SWC の ASIL

表 1 に示した安全要求について，各 SWC に割付けた図を図 5 に示す．図 5 に示したとおり，各 SWC および BSW は ASIL B であり，パーティションの設定をする必要がなかった．

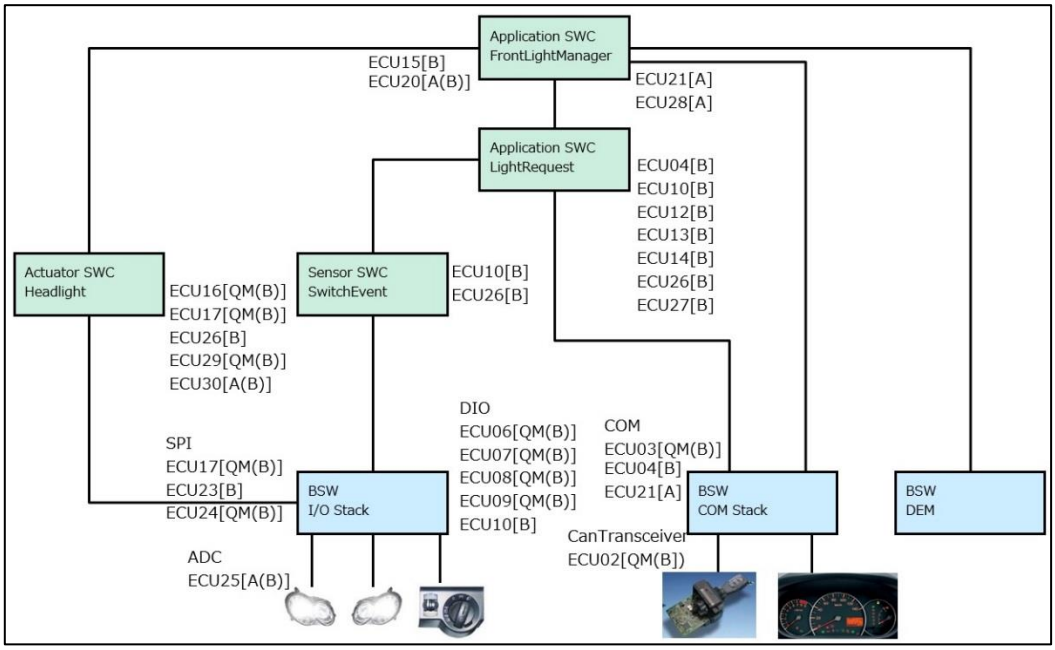

図 5 安全要求の割付け

3.3　FLM の再設計

4 つの SWC について ASIL A に変更可能か検討を行い，本書では Headlight SWC に着目した．理由として，安全要求 ECU26[B]を ASIL A にすることができれば，Headlight SWC を ASIL A に設定できると考えたためである．次に安全要求 ECU26『SWC 間で正確なデータ交換（タイミングと内容）が保証されなければならない』について，『SWC 間』を明確にした．明確化した安全要求とデータ交換で使用する機能を表 2 に示す．

表 2 安全要求 ECU26 の明確化と機能

ECU26	機能
FrontLightManager SWC から HeadLight SWC へのデータ交換が保証されなければならない	ライトの点灯／消灯
HeadLight SWC から FrontLightManager SWC へのデータ交換が保証されなければならない	ライトの監視

ここで，Headlight SWC は以下の通り，三つの機能がある．

・LB を点灯／消灯

・DRL を点灯

・LB の状態を監視

そのため，Headlight SWC の機能を三つの SWC に分割し，LB を点灯する機能を ASIL A と設定する．再設計後の SWC 名，機能，ASIL を表 3 に示す．

表 3 Headlight SWC の再設計

SWC 名	機能	ASIL
Headlight	LB の点灯／消灯	A
DaytimeRunningLight	DRL の点灯	B
Monitoring	LB の状態監視	B

再設計後の安全要求 ECU26 については，表 4 の通りとすることにした．

表 4 安全要求 ECU26 の明確化

ID	ECU の安全要求	ASIL
ECU26-1	FrontLightManager SWC から HeadLight SWC へのデータ交換（タイミングと内容）が保証されなければならない	A(B)
ECU26-2	FrontLightManager SWC から DaytimeRunningLight SWC へのデータ交換（タイミングと内容）が保証されなければならない	B
ECU26-3	Monitoring SWC から FrontLightManager SWC へのデータ交換（タイミングと内容）が保証されなければならない	B
ECU26-4	LightRequest SWC から FrontLightManager SWC へのデータ交換（タイミングと内容）が保証されなければならない	B
ECU26-5	SwitchEvent SWC から LightRequest SWC へのデータ交換（タイミングと内容）が保証されなければならない	B

また，DRL を点灯させるための安全要求がなかったため，表 5 の通り新規に追加することにした.

表 5 安全要求 ECU27

ID	ECU の安全要求	ASIL
ECU27	FrontLightManager からの要求に基づき， DRL を点灯させなければならない	B

3.4 再設計後のデータの流れ

再設計後の RTE を介したデータの流れを図 6 に示す.

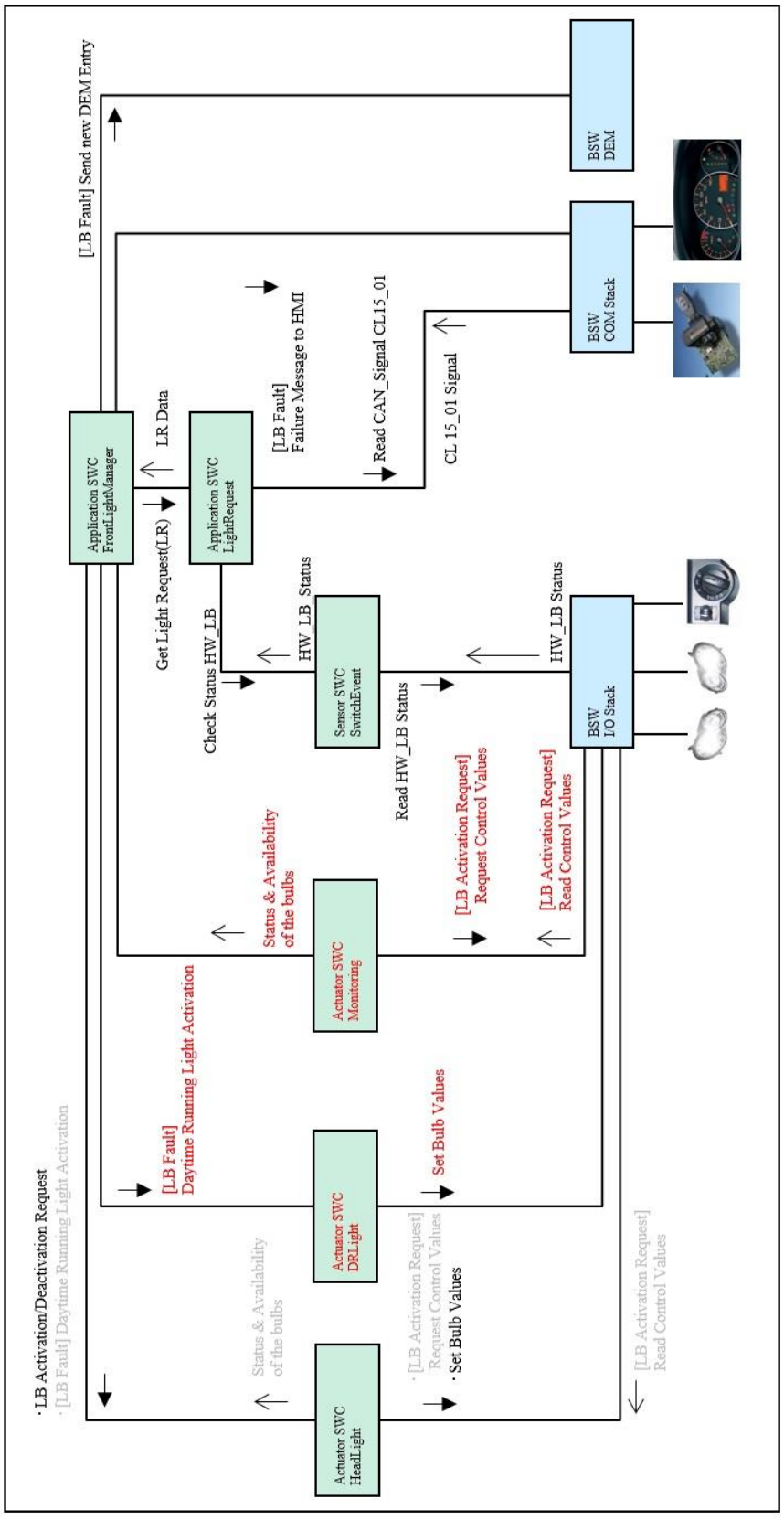

図 6 再設計後のデータの流れ

3.5　前提条件の追加

FLM システムには処理緊急度の定義がないこと，また FFI が実現できる安全要求を追加するため，前提条件の追加を行った．FLM システムの処理緊急度を下記と通り設定した．

Headlight SWC > Monitoring SWC > DaytimeRunningLight SWC
> FrontLightManager SWC > LightRequest SWC > SwitchEvent SWC

3.6　新規安全要求の追加

FFI が実現できる安全要求を追加する．追加した安全要求を表 6 に示す．

表 6 新規安全要求

ID	ECU の安全要求	ASIL
ECU100	Headlight SWC の誤作動が Monitoring SWC に悪影響を及ぼさないこと	B
ECU101	Headlight SWC の誤作動が DaytimeRunningLight SWC に悪影響を及ぼさないこと	B
ECU102	Headlight SWC の誤作動が FrontLightManager SWC に悪影響を及ぼさないこと	B
ECU103	Headlight SWC の誤作動が LightRequest SWC に悪影響を及ぼさないこと	B
ECU104	Headlight SWC の誤作動が SwitchEvent SWC に悪影響を及ぼさないこと	B

ここで，『誤動作』について，誤作動には，CPU を占有するや，他の占有領域のメモリにアクセスするなどあるが，本書では，『誤動作』を『CPU を占有する』として進める．

4. 保護の強度による分析

安全要求の分析を行う際に検討する，保護機構は強度によって二つに分けられる．

4.1 strict protection（厳密な保護）

構成要素 Y がどのような動作をしても，構成要素 X の動作にいかなる影響もないとき，X が Y から厳密な保護がされているという．この場合，影響がないため，安全要求の分析が不要となる．

4.2 safety protection（安全性の保護）

構成要素 Y がどのような動作をしても，構成要素 X の安全性に関する性質(safety property)に影響がないとき，X が Y から安全性の保護がされているという．この場合，安全要求の侵害に繋がる影響がないか，安全要求を分析することが必要となる．

4.3 保護の例

『CPU を占有する』という誤作動を例に strict protection および safety protection の説明を図 7 に示す．『CPU を占有する』ことにより⇒『処理が遅れる』⇒処理が遅れることにより『安全要求の侵害に繋がる』ことになる．ここで，strict protection の保護がなされていた場合，CPU を占有されたとしても，影響がないため，処理が遅れることはない．また，safety protection の保護がなされていた場合，処理が遅れても，安全要求の侵害に繋がることがないということになる．

図 7 保護の例

5. 安全要求の分析

5.1　新規安全要求 ECU100 の分析

新規に追加した安全要求 ECU100『Headlight SWC の誤作動が Monitoring SWC に悪影響を及ぼさないこと』について安全要求の分析を行う．

5.1.1　TP を保護機構として使用する場合

ATK2-SC3-TP の時間パーティショニング機能を保護機構として使用する場合，『CPU を占有する』という誤作動が起きても，タイムウィンドウ切り替えにより処理が遅れることがない．これは strict protection のため，これ以上安全要求の分析を行う必要がない．

5.1.2　TP を保護機構として使用しない場合

ATK2-SC3-TP の時間パーティショニング機能を保護機構として使用しない場合,『CPU を占有する』という誤作動が, 安全要求の侵害に繋がる影響がないか Monitoring SWC の安全要求に対して分析を行う必要がある． Monitoring SWC に関する安全要求について表 7 に示す．時間パーティショニング機能を保護機構として使用しない場合は，表 7 に示す安全要求の 5 件に関して，悪影響を及ぼさない根拠(表 7 の黄色ハッチングの箇所)を分析する必要がある．本書では，悪影響を及ぼさない根拠については検討しない．

表 7 Monitoring SWC に関する安全要求の分析

ID	安全要求	Headlight が誤作動することによる影響	悪影響を及ぼさない根拠
ECU20	電球に電力が供給された場合，Monitoring SWC は電球の状態（read_current_L, read_current_R）を評価しなければならない	指定されたタイミングで電球の状態を評価できない	
ECU23	ECU はフォールトトレラント時間(500ms)に対応して電球の状態測定における経路（μC HW，ECU HW，車両の配線）の故障を検知しなければならない	経路の故障を検知することができない	
ECU25	ADC は測定された電流を『read_current_L』，『read_current_R』に変換しなければならない	指定されたタイミングで電流を変換することができない	
ECU26-3	Monitoring SWC から FrontLightManager SWC へのデータ交換（タイミングと内容）が保証されなければ	FrontLightManager SWC に対し，指定されたタイミングで電球の状態を提供で	

	ならない	きない	
ECU30	電球に電力が供給された場合，Monitoring SWC は電流を読み出し，電球の状態を提供しなければならない	電流を読み出せず，FrontLightManager に対し，電球の状態を提供することができない	

5.2 新規安全要求 ECU101 の分析

新規に追加した安全要求 ECU101『Headlight SWC の誤作動が DaytimeRunningLight SWC に悪影響を及ぼさないこと』について安全要求の分析を行う．

5.2.1 TP を保護機構として使用する場合

ATK2-SC3-TP の時間パーティショニング機能を保護機構として使用する場合，『CPU を占有する』という誤作動が起きても，タイムウィンドウ切り替えにより処理が遅れることがない．これは strict protection のため，これ以上安全要求の分析を行う必要がない．

5.2.2 TP を保護機構として使用しない場合

ATK2-SC3-TP の時間パーティショニング機能を保護機構として使用しない場合,『CPU を占有する』という誤作動が，安全要求の侵害に繋がる影響がないか DaytimeRunningLight SWC の安全要求に対して分析を行う必要がある． DaytimeRunningLight SWC に関する安全要求について表 8 に示す．時間パーティショニング機能を保護機構として使用しない場合は，表 8 に示す安全要求の 1 件に関して，悪影響を及ぼさない根拠(表 8 の黄色ハッチングの箇所)を分析する必要がある．本書では，悪影響を及ぼさない根拠については検討しない．

表 8 DaytimeRunningLight SWC に関する安全要求の分析

ID	安全要求	Headlight が誤作動することによる影響	悪影響を及ぼさない根拠
ECU27	FrontLightManager からの要求に基づき， DRL を点灯させなければならない	指定されたタイミングで DRL を点灯できない	

5.3 新規安全要求 ECU102 の分析

新規に追加した安全要求 ECU102『Headlight SWC の誤作動が FrontLightManager SWC に悪影響を及ぼさないこと』について安全要求の分析を行う．

5.3.1 TP を保護機構として使用する場合

ATK2-SC3-TP の時間パーティショニング機能を保護機構として使用しない場合,『CPU を占有する』という誤作動が起きても，タイムウィンドウ切り替えにより処理が遅れることがない．これは strict

protection のため，これ以上安全要求の分析を行う必要がない．

5.3.2　TP を保護機構として使用しない場合

ATK2-SC3-TP の時間パーティショニング機能を保護機構として使用しない場合,『CPU を占有する』という誤作動が，安全要求の侵害に繋がる影響がないか FrontLightManager SWC の安全要求に対して分析を行う必要がある． FrontLightManager SWC に関する安全要求について表 9 に示す．時間パーティショニング機能を保護機構として使用しない場合は，表 9 に示す安全要求の 2 件に関して，悪影響を及ぼさない根拠(表 9 の黄色ハッチングの箇所)を分析する必要がある．本書では，悪影響を及ぼさない根拠については検討しない．

表 9 FrontLightManager SWC に関する安全要求の分析

ID	安全要求	Headlight が誤作動することによる影響	悪影響を及ぼさない根拠
ECU15	両方の電球の故障が継続的に 200ms 検出された場合，FrontLightManager は Daytime Running Light を有効にしなければならない	電球の故障を検知できない．また，検知できないため，DRL を有効にすることができない	
ECU26-2	FrontLightManager SWC から DaytimeRunningLight SWC へのデータ交換（タイミングと内容）が保証されなければならない	DaytimeRunningLight SWC に対し，指定されたタイミングで DRL を点灯できない	

5.4　新規安全要求 ECU103 の分析

新規に追加した安全要求 ECU103『Headlight SWC の誤作動が LightRequest SWC に悪影響を及ぼさないこと』について安全要求の分析を行う．

5.4.1 TP を保護機構として使用する場合

ATK2-SC3-TP の時間パーティショニング機能を保護機構として使用する場合，『CPU を占有する』という誤作動が起きても，タイムウィンドウ切り替えにより処理が遅れることがない．これは strict protection のため，これ以上安全要求の分析を行う必要がない．

5.4.2　TP を保護機構として使用しない場合

ATK2-SC3-TP の時間パーティショニング機能を保護機構として使用しない場合,『CPU を占有する』という誤作動が，安全要求の侵害に繋がる影響がないか LightRequest SWC の安全要求に対して分析を行う必要がある． LightRequest SWC に関する安全要求について表 10 に示す．時間パーティショニング機能を保護機構として使用しない場合は，表 10 に示す安全要求の 7 件に関して，悪影響を及ぼ

さない根拠(表 10 の黄色ハッチングの箇所)を分析する必要がある．本書では，悪影響を及ぼさない根拠については検討しない．

表 10 LightRequest SWC に関する安全要求の分析

ID	安全要求	Headlight が誤作動することによる影響	悪影響を及ぼさない根拠
ECU2	CAN BUS の『CAN_CL15』から論理的な『CL15_01』メッセージへの正確な変換を保証しなければならない	指定されたタイミングで『CL15_01』へ変換することができない	
ECU3	AUTOSAR BSW/ RTE を介した『CL15_01』メッセージの正しい配送が保証されなければならない．シグナル『CL15_01.CL15ON』は書き出され、正しく FrontLightManager　SWC に提供されなければならない	指定されたタイミングで『CL15_01.CL15ON』を提供することができない	
ECU4	ECU は安全目標違反につながる可能性がある，シグナル『CL15ON』に影響を与える潜在的な通信故障を検出しなければならない	通信故障を検出することができない	
ECU12	LightRequest SWC は指定された『LB_OFF』と『CL15ON』の状態を判定しなければならない	指定されたタイミングで判定することができない	
ECU13	LightRequest SWC は『LB_OFF』，『CL15ON』，指定されたタイミングに基づきライト要求条件を解析しなければならない	指定されたタイミングでライト要求条件を解析することができない	
ECU14	LightRequest SWC は『LB_OFF』，『CL15ON』の解析結果に基づいて，ライト点灯要求をセットまたはリセットしなければならない．『CL15_01』メッセージの通信故障が 200ms 以上継続的に検出された場合，および『LB_OFF』の故障が 200ms 以上継続的に検出された場合，ライト点灯要求をセットしなければならない．	指定されたタイミングで通信故障を検知することができない．またライト点灯要求をセットできない	

ECU26-2	LightRequest SWC から FrontLightManager SWC へのデータ交換（タイミングと内容）が保証されなければならない	FrontLightManager SWC に対し，指定されたタイミングでライト点灯要求を出せない	

5.5　新規安全要求 ECU104 の分析

新規に追加した安全要求 ECU104『Headlight SWC の誤作動が SwitchEvent SWC に悪影響を及ぼさないこと』について安全要求の分析を行う．

5.5.1 TP を保護機構として使用する場合

ATK2-SC3-TP の時間パーティショニング機能を保護機構として使用する場合，『CPU を占有する』という誤作動が起きても，タイムウィンドウ切り替えにより処理が遅れることがない．これは strict protection のため，これ以上安全要求の分析を行う必要がない．

5.5.2　TP を保護機構として使用しない場合

ATK2-SC3-TP の時間パーティショニング機能を保護機構として使用しない場合,『CPU を占有する』という誤作動が，安全要求の侵害に繋がる影響がないか SwitchEvent SWC の安全要求に対して分析を行う必要がある． SwitchEvent SWC に関する安全要求について表 11 に示す．時間パーティショニング機能を保護機構として使用しない場合は，表 11 に示す安全要求の 3 件に関して，悪影響を及ぼさない根拠(表 11 の黄色ハッチングの箇所)を分析する必要がある．本書では，悪影響を及ぼさない根拠については検討しない．

表 11 SwitchEvent SWC に関する安全要求の分析

ID	安全要求	Headlight が誤作動することによる影響	悪影響を及ぼさない根拠
ECU06	入力『HW_LB_OFF』の正確な読出しを保証しなければならない	指定されたタイミングで読み出しを行うことができない	
ECU10	ECU は安全目標違反につながる可能性がある，『LB_OFF』に影響を与える潜在的な故障を検出しなければならない	故障を検出することができない	
ECU26-5	SwitchEvent SWC から LightRequest SWC へのデータ交換（タイミングと内容）が保証されなければならない	LightRequest SWC に対し，指定されたタイミングでスイッチ状態を提供することができない	

6. TP 機能が有効な点

ATK2-SC3-TP の時間パーティショニング機能を保護機構として使用する場合，『CPU を占有する』という誤作動による安全要求の分析が不要であることがわかった．それに対し，ATK2-SC3-TP の時間パーティショニング機能を保護機構として使用しない場合，誤作動が安全要求の侵害に繋がる影響がないか，各 SWC の安全要求 18 件に対し分析が必要であることがわかった．この安全要求 18 件分の分析の差が TP を使用する上で有効な点であるといえる．

7. 参考文献

・AUTOSAR 『Safety Use Case Example』AUTOSAR Release4.2.2
・Certification Authorities Software Team 『Position Paper CAST-2』

8. 変更履歴

Version	Date	Detail	Editor
1.0.0	2017/03/24	新規作成	NCES