安全関連システムのRAMSによる管理の考え方とその適用

吉永　純*

1. 鉄道のRAMSについて

1.1　RAMSの概要

RAMSは，Reliability（信頼性），Availability（アベイラビリティ），Maintenability（保守性）のRAMと，Safety（安全性）の4要素を表すもので，鉄道分野向け機能安全規格，IEC 62278「RAMS」の通称である。

「鉄道RAMS」と呼ぶべきかもしれないが，他にRAMとSafetyを併記した国際規格は無く，世界的にも定着しているため，本稿ではRAMSと表記する。

RAMSは，鉄道製品に要求されるRAM及びSafetyの4要素に関する要求事項を実現し，かつ実証（すなわち根拠のある説明ができること）するための手順を定めている。海外の鉄道プロジェクトでは急速にデファクト化し，安全上重要な製品にはRAMSへの適合性が要求されている。

しかし，鉄道にはIMOに相当する国際的な枠組みは無く，一部の国を除いて法的な義務もないため，当事者間の仕様書でRAMSの適用を決めるのが一般的である。日本国内の案件ではRAMSが要求されることは無いものの，RAMSを活用できる鉄道製品メーカーは徐々に増えている。

RAMSは，鉄道分野以外の機能安全規格と比べ，安全性（S）を重視しつつも，RAM及びSafetyの各ファクター間及びライフサイクルコスト（LCC）とのバランスの重要性に言及されている点が特徴的である。

本稿では鉄道のRAMSを例として，RAMSの管理手法によるメーカー及びユーザーの製品開発及び製品使用時の管理法や，従来のトラブルゼロを目指す考え方との違いなど，特徴的な点を述べる。

1.2　RAMSが広がる理由

海外の鉄道事業者の立場では，想定外のリスクが生じない安全な製品を調達するため，メーカー（インテグレータを含む。）にRAMSに適合した手順で，着実な製品開発を行うことを求めている。

このRAMSによる製品開発を大づかみして頂くため，椅子の開発を例示したい。なお，RAMSは本来，プログラムを内蔵した製品を対象としている。

一般的に椅子を開発する時，基本形状を考えた上で，足の強度や材質を検討するのではないだろうか。

これは「荷重による破損」リスクに対し，「どれだけの荷重に耐えればよいか」と目標を考え，「その値以上の強度を持たせる」と，リスクへの安全対策を頭の中で検討している，と考えられる。

図1では3種類の椅子を作ろうとしているが，直観的に（2）や，可動部のある（3）の椅子には多くの危険性（リスク）を挙げられると思う。次に，これら挙がったリスクへの安全対策を考えていく。

（3）の椅子に懸念される「指を挟む」リスクに，「異物検知機能（センサー）」が不可欠な対策と考えた場合，高額な高信頼性センサーを選ぶのは，おそらく早計である。むしろ，手頃な価格のセンサーを複数使って，見逃しを防ぐ機構としたほうが合理的なためである。このような検討が，RAM及びSafetyの4要素のバランスの考慮に該当する。

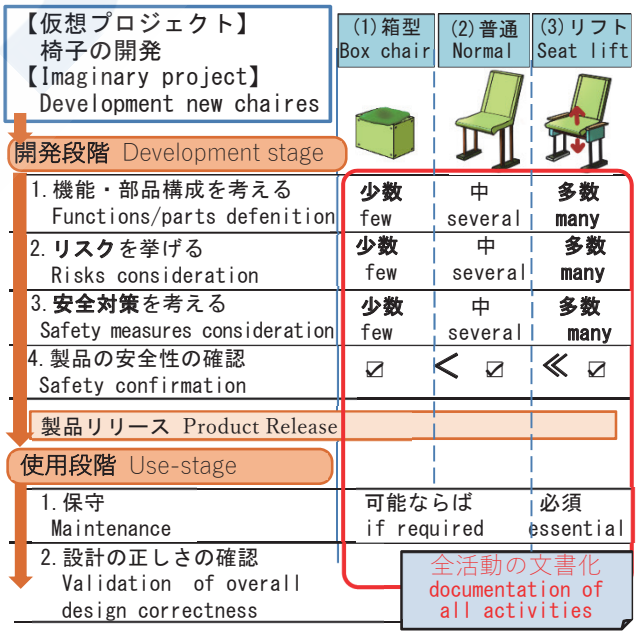


図1　リスクベースの製品開発イメージ

安全対策はハードウェア，ソフトウェアに限られず，ユーザーの使用方法，定期点検等，さまざまに

*　独立行政法人自動車技術総合機構　交通安全環境研究所　交通システム研究部　研究員（元国土交通省鉄道局　車両工業企画室長）

対策する。しかし，それでも残る一定水準以下のリスク（残存リスク）は，許容する。RAMSでは，上記の一連の検討は部品や機能ごとに，計画に従った手順で進め，要所では実施結果を多層的に検証する。最終的に，すべての活動の計画，実行，判断材料等を文書化し，立証資料とする。

RAMSなどの機能安全規格の手順では，複雑な機能をもつ製品ほど作成する文書量は増大するが，RAM及びSafetyに関する要求事項に対して十分な検討や対策を，機能安全規格に基づいて開発を行ったことを立証できる。また，ユーザーとメーカーの責任範囲も明確になる。

これに対し従来の手法は，例えば，「家具のガイドラインに整合している」のように，技術基準等への適合性により一定の安全性が示せるが，技術基準等が想定するリスクの範囲は明確ではない。

海外案件では，製品ユーザーが必ずしも専門家ではないため，安全と言える根拠や，RAMの見通しを説明する必要がある。メーカーの常識はユーザーの常識ではないため，もし誤解があると後々トラブルとなることから，RAMSで製品が想定しているリスクの範囲や判断根拠，メーカーとユーザーの責任分担の分かる文書の作成が要求されており，これら文書で確認できることが重要となる。

椅子の例では，万一事故が生じた際，これら文書によりメーカーの開発過程で安全要求事項及びRAM要求事項を満たし（**図2**），機能安全規格に従った手順で開発したシステムだ，と安全性の根拠を機能安全規格に求めることができる。また，事故の原因究明も客観的に行える。

一方，従来手法では，開発手順の拠り所はISO 9001ベースとなり，手順の妥当性を示すことには労力を要すると思われる。

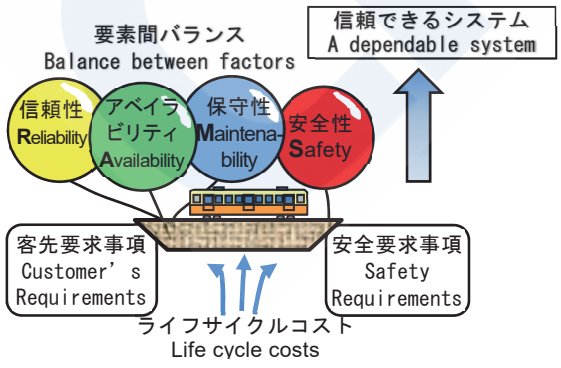


図2　機能安全を拠り所としたシステム開発

2. 機能安全規格

2.1　概要

ここまで述べてきた機能安全とは，安全に関係するシステム・装置の安全性を保つための手法の1つである。機能安全では，システムや装置には何らかのリスクが内在していると考える。故障や人為的なミス等によってそのリスクが顕在化した場合にも，許容できないような被害は生じないシステム・装置を「安全機能（safety function）」により実現することで，安全を確保する手法である。

国際規格IEC 61508シリーズ「電気・電子・プログラマブル電子系（E/E/PE）安全関連系の機能安全」が発行され，国内ではJIS C 0508が対応している。

日本でも，従来は安全基準への適合性によって安全性を確認していた装置が，IT技術により複雑化，リスクが見えにくくなったことに伴い，安全性の立証に機能安全を適用するケース[1)]など，新たなリスクマネジメント手法として利用され始めている。

2.2　産業分野別の機能安全規格

機能安全規格IEC 61508は，全産業向けの安全機能に使用されるE/E/PEが対象で，メーカーやユーザも適用対象であり，抽象度の高い語句で記述されているため業務のイメージをつかみにくい。

そのためRAMSのような，特定の産業分野向けに，検討すべき指標や開発段階が製品の特長に合わせた機能安全規格の開発が進められている（**表1**）。船舶分野に対する規格は，現状では発行されていない。

表1　機能安全規格の体系[2) 3)]

分類	該当規格の例
基本安全規格 Basic safety publication	IEC 61508(JIS C 0508) 機能安全
グループ安全規格 Group safety publications	IEC 62278 鉄道RAMS IEC 62279 鉄道ソフトウェア安全 ISO 26262 自動車電子制御 IEC 62061 産業機械類 ISO 13849 機械類の制御システム安全関連部 IEC 61513 原子力分野

3. RAMSの考え方

3.1　製品ライフサイクルの品質管理

機能安全では，製品の構想段階から使用終了段階まで，製品ライフサイクルをフェーズに分け，各フェーズで行うべき要求事項を規定する。

IEC 61508の場合は16段階，RAMSでは一部の段階を統合しているため14段階だが，詳細は割愛する。

ライフサイクルの各段階を一般化し，かつ，大く

くりすると図3の点線部のように3つに分類できる。

製品のリリースは，「設計段階」と「営業段階」の間にあたる。リリースをもって製品開発業務が一段落し，点検修理等のアフターセールスの範疇となることが一般的と思われるが，RAMSの場合，リリースの後のRAMやSafetyに関して行う活動も製品開発の一連の業務として，一貫した活動計画をメーカーが事前に作成することを要求している。

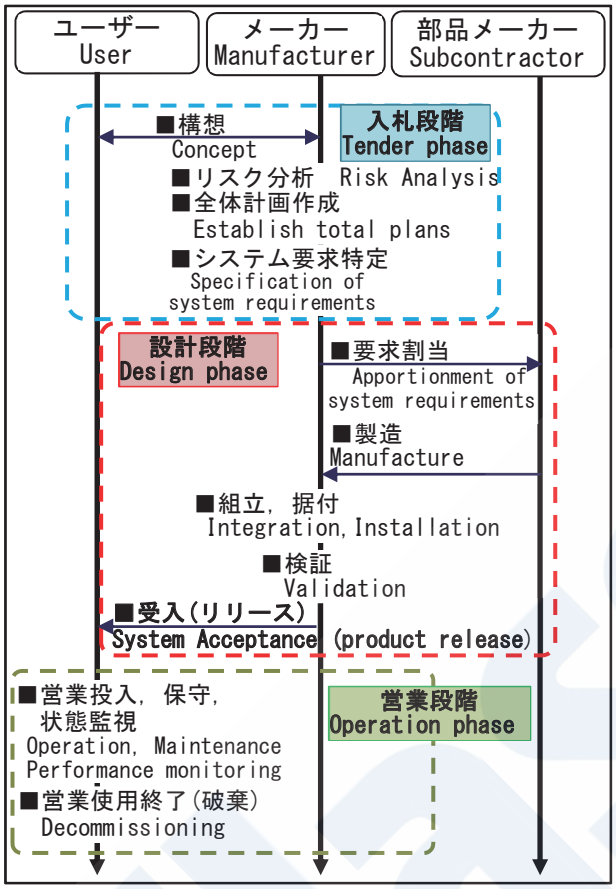


図3　製品ライフサイクルにおける活動

作成する計画は，安全性は「Safety Plan」，RAMは「RAM programme」と呼ばれるが，実際の書類名は任意である。両計画とも，製品の目標，達成のための方策，人員体制，設計・製造・検証方法や作成する文書等の管理活動を計画する。

さらに，営業段階において，設計時に算出したRAM目標の状況確認方法，設計時に前提としたメンテナンス方法も記述される。これらは後述するように，ユーザーに引き継がれる情報となる。

こうしたRAMSに基づく活動は，組織の品質管理システムと関連して実施することがRAMSの必須要求（“shall” requirement）であり，品質管理システムはRAMSにおいて重要な位置付けである（図4）。

両計画とも製品設計開始前に作成され，大枠的事項が書かれるが，RAMSではライフサイクル全体を通じた首尾一貫した計画があることが重視される。なぜなら計画すれば計画の実施をチェックでき，計画に無い手順による勝手な仕様の追加や修正等無秩序な活動が行えないこと（無秩序な行動は，妥当性確認ができず，潜在リスク増大の可能性がある），ユーザーへ必要情報を漏れなく伝えられることなど，製品ライフサイクル全体にわたって品質を管理できるためである。3.2.2に後述するように，ソフトウェアの品質確保の上でも重要な考え方となっている。

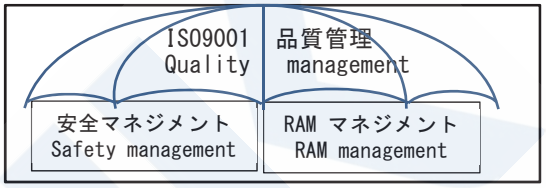


図4　品質管理の下での安全性保持

3.2　故障の種類と対策

RAMSでは，故障（failure）には以下の2種類があり，その特徴に適した対策を行う（図5）。現状多くの装置がソフトウェアを内蔵する（E/E/PE）と考えられるため，その場合，両方の対策が必要となる。

(1) ランダム故障：確率的に発生する故障
(2) システマティック故障：特定の入力の組み合わせ又は特定の環境条件下で発生する故障

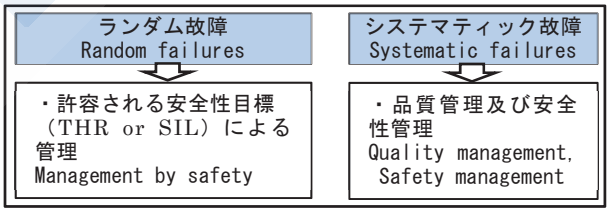


図5　故障の種類と対策

3.2.1　ランダム故障対策

ランダム故障は，ハードウェアの施工不良や劣化等により確率的に発生する。影響評価は深刻度と発生率によるため，どのようなハザードが，どの程度の深刻度・発生率（リスク）で起こるかが重要となる。

そのため，ランダム故障に対しては図6のように，ハザードごとに（この図では「ガイド機能の喪失(脱線)」），システムに必要となる目標（許容される故障率目標，THR：Tolerable Hazard Rate又はSIL：Safety Integrity Level）をサブシステムに割り当て，この目標を達成すべく安全対策を行う。割り当てた目標はサブコントラクターに伝達することで，システム全体の性能を守る。

実務上は，THRを表2により換算したSILを用いる場合が多い。また，サブシステムが決まっている場合，サブシステムの故障率目標を先に決める場合もある。

割り当てにあたっては，個々のサブシステムに必要以上の高い目標を割り当てることは，不必要な複雑化やコスト要因となるため，合理的に割り当てることが，バランス重視のRAMSにかなっている。

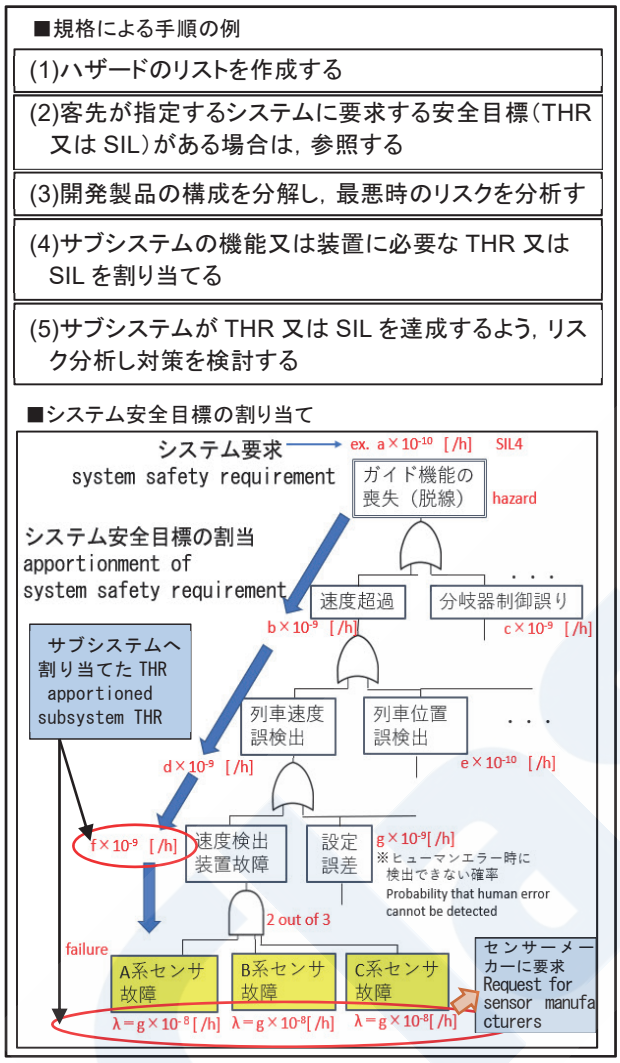


図6　サブシステムへのTHR割当の例

表2　THRとSILの換算

安全機能の目標とする危険側故障率の平均値	対応SIL
1×10^{-8} [/h]　未満　～　1×10^{-9} [/h]	SIL 4
1×10^{-7} [/h]　未満　～　1×10^{-8} [/h]	SIL 3
1×10^{-6} [/h]　未満　～　1×10^{-7} [/h]	SIL 2
1×10^{-5} [/h]　未満　～　1×10^{-6} [/h]	SIL 1
～　1×10^{-5} [/h]	SIL 0

出典：IEC 61508-1 Ed.2.0　Table 2を一部改変
備考：要求（高頻度）に応じ稼働するE/E/PEシステム及び連続稼働するE/E/PEシステムの場合である。

3.2.2　システマティック故障対策

システマティック故障は，典型的にはソフトウェアのバグや，作業指示ミスによる設計間違いのような作り込まれたものである。特定条件が揃うと必ず発生し，確率的に生じるものではない。

このような故障への対策として，前述の許容される故障率目標（THR）にふさわしいマネジメントや，技法（Techniques and Measures。以下「技法」という。）を適用することで，作り込みの防止や，人為ミスを検査等で検出するといった対策を行う。

マネジメントに関しては，能力のある者による段階ごとの検証（Verification）や妥当性確認（Validation）が特徴的である。技法に関しては，表3のRAMSの関係規格の例のような，いわば，このSIL目標の製品を製作する場合，このような対策が必要，というノウハウを示すもので，SILが高いほど要求は多くなる。

従来手法で開発された製品の場合，規格に書かれる技法とは完全には一致しないため，製品品質は優れていても規格と不整合，という事態が生じる。回避するためには，今後の開発時には，極力機能安全規格の技法と整合させ，相違の生じる点は，その理由を記録しておくことが重要である。

表3　規格の技法の例

技術・手法 Technique/Measure	SIL0	SIL1	SIL2	SIL3	SIL4
4. 機能試験の実施 Functional testing	M	M	M	M	M
5. チェックリストで確認 Checklists	R	HR	HR	M	M
9. レビューアーによる検証 Walkthrough	R	R	R	HR	HR

凡例：M:義務(Mandatory)，
HR:強く推奨(Highly Recommended)，
R:推奨(Recommended)
出典：IEC 62279 Ed2.0　Table A.11(抜粋)

3.2.3　安全に関するリスク分析

機能安全規格の「安全」は，機能安全規格ごとに差異があるが「許容できないリスクがないこと（freedom from unacceptable risk）」と定義される。

リスクは，「危害の発生確率とその危害の程度の組み合わせ（combination of the probability of occurrence of harm and the severity of that harm）」と定義される。発生頻度が高く，かつ危害の程度が重篤なほど高いリスクとなる。許容できるリスクかどうかは極めて重要で，既存品の実態調査等，何らかの根拠から適正に決定することが，バランスのよいシステムの実現に不可欠である。

反面，対策を講じてもなお残るリスク（residual

risk）（**図7**）は，社会的に許容（tolerable）されると判断できるリスクは製品への残存を許容し，0にしない。

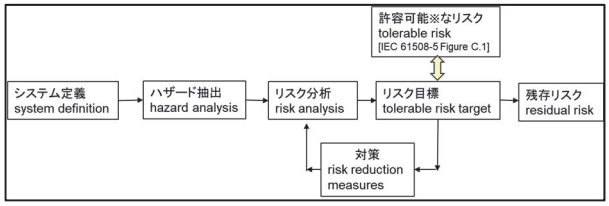


図7　リスク縮減フロー

表4は，リスクの発生頻度と被害の深刻度のマトリクスである。メーカーでは，発生頻度や深刻度を具体的に決め，**表5**，**表6**のようなFMEA解析により少なくとも「望ましくない」「許容できない」範疇のリスクを除去又は軽減する対策を行う。欧州のメーカーでは，FMEA解析では**表5**に加え，その部品に適した保守方法も合わせて検討されている（5.1に後述）。

リスクの発生頻度のレベル分けやFMEAを行うためには，現状の故障率が欲しいところだが，この把握はメーカー各社とも苦労している。さらに，不幸にしてリスクが顕在化するのは営業段階のため安全関係の法令の規制対象となるが，法令やRAMSには社会的に許容される水準は示されておらず，ユーザーの要求事項やALARP原則[4]等を参照し，メーカーが安全性やRAMについて，目標を決める必要がある。

これらは，**図8**のsafety caseという文書にまとめる。

関係者への立証に用いる観点からは，考えられるリスクは取捨選択をせず淡々と計上することが望ましい。さらに，リスクへの対策，判断根拠，ユーザーの要求事項等を文書上でつながりを追える（トレースという）必要もある点が独特な点といえる。

表4　安全性のリスク評価マトリクス

危険な事象の発生頻度	リスクの程度			
頻繁に発生	望ましくない	許容できない	許容できない	許容できない
発生の可能性大	許容できる	望ましくない	許容できない	許容できない
時として発生	許容できる	望ましくない	望ましくない	許容できない
いつか発生	無視できる	許容できる	望ましくない	望ましくない
発生しそうもない	無視できる	無視できる	許容できる	許容できる
考えられない	無視できる	無視できる	無視できる	無視できる
	軽度	許容限界	重大	深刻
	結果の深刻さの程度			

出典：IEC 62278:2002 Table 6　より抜粋

表5　Functional FMEAの例

ID	装置/機能 ITEM/Function	フォールト Fault	生じる事象 Fault consequence	既存の対策 Existing Measures
R1	Invertor	current v data loss	halt	warning
	・・・			

表6　Design FMEAの例

ID	装置/機能 ITEM /Function	フォールト Fault	対策前 Potential			対策後 Result			
			重篤度 Sev	頻度 Occ	評価 RPN	対策 Mitigation	重篤度 Sev	頻度 Occ	評価 RPN
M1	Invertor	current v data loss as a result of wrong input	2	3	6	add input data rationality check function	2	1	2
	・・・								

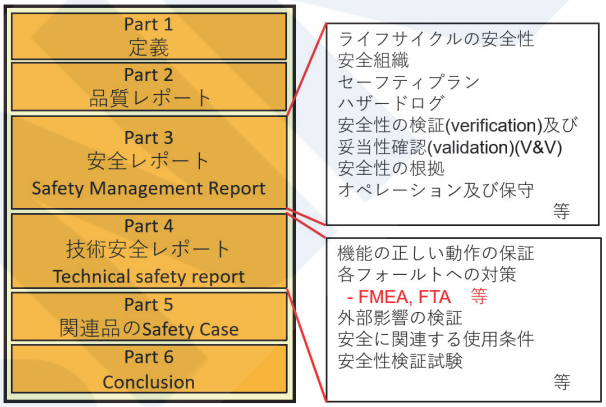


図8　安全性立証書類safety caseの構成

4. RAMの管理の考え方

4.1　RAMの要素

製品ユーザーは，製品のSafetyは当然のものとして，ライフサイクルコストに関わるRAMを重視している。鉄道車両は特にRAMが重視されるため，具体的な数値が書かれた調達仕様が見受けられる。

RAMの各要素について，具体的な指標に関する規定はなく，いくつか例示だけのため（例：CLC/TR 50126-3，EN 50657），製品に適した指標が選ばれる。主なものを**表7**に列記する。

例えば「列車の不稼働頻度　5［分／年］」ならば，アベイラビリティ要求9.5×10^{-6}（9.5×10^{-4}［%］），「列車運行が停止する故障　2件／10万［車両走行km］」なら，MTBF（深刻な故障）=50,000［車両走行km］が要求されていることとなる。

同表中のλは故障率である。安全性の面では危険側に作用する故障率が重要で，さまざまな分類方法があるが，ここではλ_S（安全側故障率）とλ_D（危険側故障率）により，次の式(1)のように定義し表中で使用している。

故障時に安全側に動作するよう設計する「フェー

ルセーフ」は，λ_Dの割合を下げる工夫をしたアーキテクチャとも言える。

表7　RAM及びSafetyの指標

	概要	主な指標
信頼性(R)	要求された機能を，失敗することなく，所定の時間動作させることができる能力	MTBF [h]，MDBF[km]（平均故障間隔），$\frac{1}{\lambda_S+\lambda_D}=\frac{1}{\lambda}$ [1/h]
アベイラビリティ(A)	部品やシステムが，要求された機能を，ある瞬間又は所定の時間動作させることができる状態にしておける能力	$\frac{MTBF}{(MTBF+MTTR)}$ [%] $\frac{\mu}{\lambda+\mu}$ [%]
保守性(M)	所定の条件で使用されている製品を，所定の時間内にメンテナンスすることが出来る可能性	$\mu=\frac{1}{MTTR}$ [%]，MTTR [h]（平均修理時間）
安全性(S)	許容できないリスクがないこと	λ_D [1/h]（危険側故障率），MTBF-H [t]（平均ハザード発生間隔）

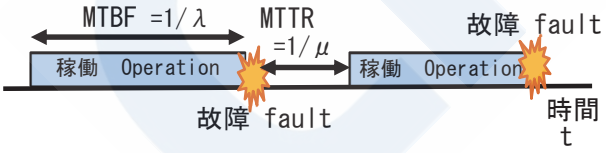
表中において

$$\lambda=\lambda_S+\lambda_D \qquad (1)$$

ただし$0\leq\lambda\leq1$を満たす時間的一定値

MTBF，MDBFは**図9**のように，故障が発生する平均時間又は平均列車走行キロを表す。例えばMDBF＝100,000kmのシステムは，平均10万km走行ごとに1件故障が発生することを意味する。

表中のMTTRは，修理又は交換が前提のシステムで，修理手配や保守部品手配も含む，故障から修理完了までの時間を表す。



MTBF(Mean Time Between Failure)：平均故障間隔[h]
MTTR(Mean Time To Repair)　　：平均修理時間[h]

MTBF:MTTRが9:1のとき，アベイラビリティ(A)=0.9
MTBF:MTTR=9:1 , Availability=0.9

図9　平均故障間隔の概念

MTTRの逆数μは，単位時間当たりの修理完了率［1/h］で，保守の完了までの時間が確率的な場合に適している。故障後すぐに修理できる場合も，深夜まで待って修理する場合もある鉄道車両では，例えばMTTR=20h（μ=1/20），というように，製品の保守性の目標を立てるのに使われる。

以上まとめると，信頼性（R）はシステムが機能する時間や距離，アベイラビリティ（A）はシステムが全時間のうち稼働している割合，保守性（M）は故障後に修理に要する時間又は修理される確率（正味の保守時間に加え，移動時間も含む）を表す。ただし他の指標もありえる。

なお，保守性についてはここでは主に修理としているが，製品特徴によっては，定期点検，塗油，摩耗品交換，清掃作業まで含める場合もある。

4.2　RAM目標の設定と割り当て

前掲の**図6**においてSafetyのシステム要求の割り当てを述べたが，RAMのうち特に信頼性（R）については客先要求がある場合，メーカーがシステム目標値を決め，次にサブシステムへ割り当てを行う。

このときFTAは複雑すぎるため，IEC 61078による信頼性ブロックダイヤグラムで論理構造を単純化し，システム全体の信頼性を計算する（5.2参照）。

また，解析された信頼性の適否を評価するため，前掲の**表4**（リスク評価マトリクス）と同様に，信頼性についても，故障の深刻さと発生頻度を，メーカーにおいて定義を行う。

表8は鉄道車両に搭載する部品に関するリスク評価項目の例である。鉄道車両部品のため，機能の維持状況を判断基準としている。頻度については，はMTBF（又はMDBF）が使われることが多いが，安全性への影響度合い，影響の波及範囲など，把握しやすく，ユーザーに分かりやすい分類が行われる。

表8　信頼性のリスク評価例

深刻さ	システムの故障モード	運行への影響
深刻	全体故障	運行不能
大きい	許容限界の機能故障	応急的運行
小さい	許容限界に達しない機能故障	応急的運行
無視	無視できる程度の機能故障	正常運行

アベイラビリティ（A）については，前掲の**表7**のように信頼性，保守性と密接な要素のため，アベイラビリティの目標は信頼性・保守性の目標達成により達成する関係にある。

保守性（M）については，システム，サブシステムごとに，**表9**の保守の種類のどれをどのような頻度で適用すべきかを，保守コストやMTTR，安全性への関与度合いから判断した目標を設定する。

RAM及びSafetyの各要素は相互に密接である。繰り返し検討することで各要素の目標を達成する。

表9　主な保守の種類

保守の種類 type of maintenance	概要 Outline
予防保全 Preventive maintenance	期間や走行距離などの一定周期を定め，保守作業を行う
事後保全 Corrective maintenance	故障や不具合を検知した場合に保守作業を行う
状態監視保全 Conditioned based maintenance	状態監視を行い，あらかじめ定めた指標値に達した場合に保守作業を行う

5. RAM及びSafetyのバランスの適用例

近年，状態監視技術や記憶デバイス等の汎用部品の信頼性が向上している。本章では，安全性に実質影響せずに一般品活用等によるRAMの検討について例示する。

5.1　信頼性と保守性

センサー技術の発達により，従来は一定期間で交換していた部品を，故障の予兆検出時に交換する「状態監視保全」への転換が進んでいる。

図10のように故障の予兆を検出してから故障までの時間（P-Fインターバル）内で異常を検知し，保守が可能なら合理的なため，異常を検出しやすい特性をもつ機械装置に取り入れられている。

この方法は，高い安全性が求められる装置には不向きだが，その他のシステムでは，大改修せず，保守でシステムのMTBFを延ばすことが可能となる。

欧州のメーカーの場合，システムの設計時に異常の検出・表示機能の信頼性を検討した上で，部品に適した保守方法と周期を前掲の表5のFunctional FMEAに合わせて記載する等，保守を活用したシステムの信頼性向上策が戦略的に行われている。

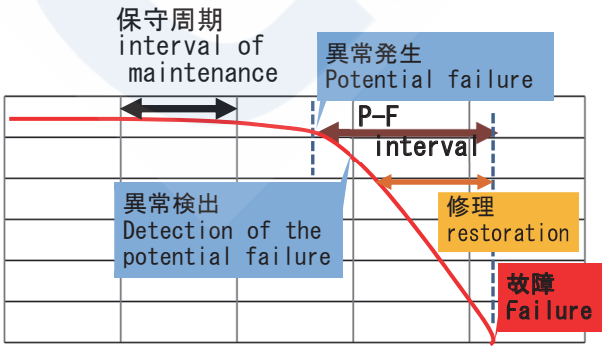


図10　P-Fインターバル内での保守

5.2　安全性と信頼性

図11は，安全関連システムで用いられる，同一装置を冗長に接続する構成を示している。2/3冗長系システムは多数決論理で2台の出力が一致した場合に採択，待機二重系システムは故障検知時に待機する一系にSW（スイッチ）で切り替える，安全対策である。

図12では，2/3冗長系システムを構成する装置A，B，Cの故障と，システム全体の故障（機能の停止の状態，failure）を図示している。

装置A，B，Cは故障率λ，修理率μ，危険側故障率λ_Dの同一装置で，スイッチ（SW）2台のいずれかの故障率を（1-p）と表せる時，安全性に影響せずに一般部品による低コスト化を狙ったシステム検討の考え方の例を示す。

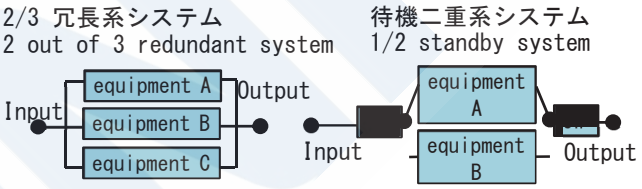


図11　ブロックダイヤグラム

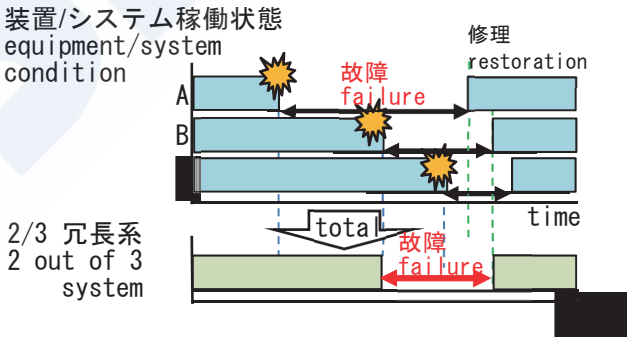


図12　2/3冗長系システムの故障

2/3冗長系システムの安全性$S_{2/3}$は，同時に2台以上が危険側故障を生じる場合以外の確率であるため式(2)，待機二重系システムの安全性$S_{1/2s}$は，スイッチ故障と，機器の危険側故障時のため，式(3)のように表せる。

$$S_{\frac{2}{3}} = 1 - \left(\lambda_D{}^3 + {}_3C_2\lambda_D{}^2(1-\lambda_D)\right) = 2\lambda_D{}^3 - 3\lambda_D{}^2 + 1 = (2\lambda_D + 1)(1-\lambda_D)^2 \quad (2)$$

$$S_{\frac{1}{2s}} = 1 - \left(p \cdot \lambda_D + (1-p)\right) = p(1-\lambda_D) \quad (3)$$

λ_D：装置の危険側故障率
dangerous failure rate of equipment[1/h]
p：スイッチが2台とも故障していない割合
inverse of failure rate of two switches[1/h]

一方，信頼性(1/λ)については，米国空軍の研究機関の文献[5]より，2/3冗長系の故障率$\lambda_{2/3}$は式(4)，待機二重系の故障率$\lambda_{1/2}$は式(5)のように表せる。

$$\lambda_{(n-q)/n} = \frac{(n)!\ \ (\lambda)^{q+1}}{(n-q-1)!\,(\mu)^{q}} \qquad (4)$$

$$\lambda_{n/n+1} \qquad = \frac{n[n\lambda + (1-p)\mu]\lambda}{\mu + n(p+1)\lambda} \qquad (5)$$

n：稼働中の機器数（この場合n=3）
number of active units (n=3,this case)
q：故障してもシステムが動作する機器数（この場合q=1）
number of units allowed to fail (q=1,this case)
μ：修復率
repair rate[/h]
p：スイッチ×2台とも故障していない割合
inverse of failure rate of two switches[1/h]

式(2)から式(5)により，**表10**に，高信頼品ではあるが修理手配に時間がかかる部品を使ったシステムと，一般製品のため手配が容易だが，故障率が高い製品を使うシステム（いずれも仮想である）について，仮想の数値により，システムごとの信頼性及び安全性を算出した。

表10　安全性と信頼性の試算例

	高信頼品 high reliable equipment	一般品 normal equipment
装置単体のパラメータ Parameters of single equipment	λ=1×10^{-5} λ_D=1×10^{-7} μ=1/24 =4.17×10^{-2} p=1-10^{-5}	λ'=5λ =5×10^{-5} λ_D'=10λ_D =1×10^{-6} μ'=1/4 =2.5×10^{-1} p'=p=1-10^{-5}
2/3冗長系システム 2 out of 3 rendant system	$\lambda_{2/3}$=1.44×10^{-8} $s_{2/3}$=1-3×10^{-14} （SIL 4に相当）	$\lambda_{2/3}'$=6.00×10^{-8} $s_{2/3}'$=1-3×10^{-12} （SIL 4に相当）
待機二重系システム 1 out of 2 standby system	$\lambda_{1/2}$=2.50×10^{-9} $s_{1/2}$=1-1×10^{-5} （SIL 1に相当）	$\lambda_{1/2}'$=1.05×10^{-8} $s_{1/2}'$=1-1×10^{-5} （SIL 1に相当）

注：表中の数字は仮想のものである.
Remarks: All figures in the above table are virtual

一般品の故障率は高信頼品より5～10倍高い（悪い）想定で算出しているが，アーキテクチャによって高信頼品を用いるシステムと同等の値を示す一般品があることが分かる。

信頼性向上への寄与度が大きい要素は，一般品の修理率μを24時間から6時間に短縮したことであり，修理率の改善はRAM要素の改善に効果的である。

5.3　ライフサイクルコスト（LCC）の算出

RAMSでは，LCCに関し，コストで安全性を決めてはならないこと，RAM及びSafetyとのバランスの重要性へ言及があるが，具体的な要求事項は無い。

しかしLCCは，ユーザーがRAM目標を決定する際の強い関心事項のため，欧州では，業界団体が欧州域内で調査した実績値をバックデータとした計算ツールが開発されている（**図13**）。

詳細な条件を入力するほど精度が増す構造であり，メーカー，ユーザーが広く共有し活用されている。

日本にはこうしたツールはなく，メーカー各社が独自に取り組んでいる。メーカー1社で把握することは難しく，業界として取り組むことが望ましいが，ユーザーの営業上の機微情報でもあるため，不可欠ではあるが，難しい課題となっている。

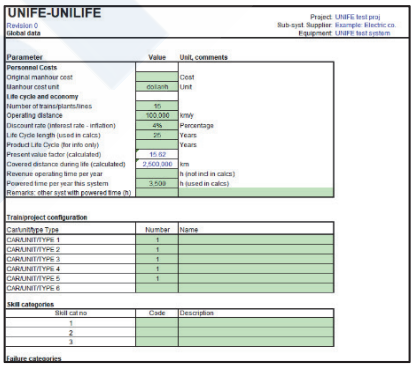


図13　LCC計算ツール「UNILIFE」

6. RAMSでのユーザーの役割

製品をリリースされたユーザーは，SRAC（Safety Related Application Condition）と呼ばれる，メーカーからユーザーへの技術的な依頼事項をまとめた書類に従い，製品を使用する。

SRACは使用説明書と似ているが，SRACはメーカーのリスク分析結果を踏まえて作成されるもので，リスクの防止の観点で首尾一貫した，製品のリスクを顕在化させないために必須の使用条件が記載されたものである。メーカーが作成するセーフティケースにも含まれ，ユーザーに交付される。

またユーザーには，**図14**の緑色のサイクルで示す，FRACAS（Failure Reporting, Analysis and Corrective Action System）というフィールドデー

タ分析を定期的に行うことが推奨されている。日常の保守や運行で把握した故障等（同図中の紫色）や運行データから，RAM目標の実現度を監視する。

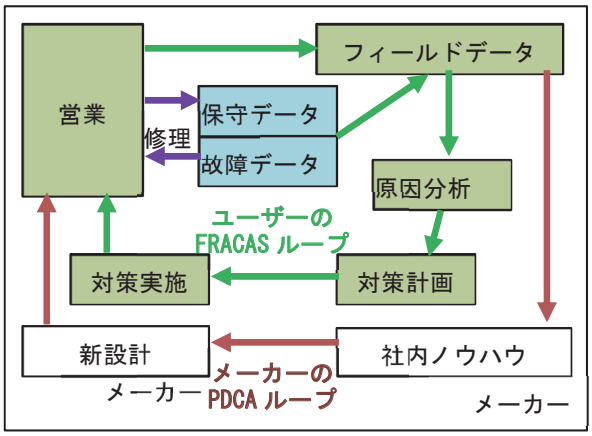


図14　ユーザーのFRACAS分析によるPDCA

その結果，もし解離が見られる場合には何らかの不具合又はリスクの顕在化も懸念されるため，原因の分析調査や，対策を実施し改善を行う。

一方メーカー側では，ユーザーからの連絡や，自身の品質マネジメントシステムの活動として，製品の設計段階で検討したRAM及びSafety指標が達成されているか調査する。

この過程でもし新たなリスクを検出した場合には，ハザードログという製品のリスクデータの更新を行い，今後の製品開発に活かすPDCA活動を行う。

製品の故障発生は，バスタブカーブとして広く知られるように，初期故障が多い状態から徐々に低下していき，やがて故障発生率が低く安定した状態に至る。そのため，海外の鉄道プロジェクトでしばしばみられる，要求未達成時に課す高額なペナルティ（製品に要求した信頼性目標を達成していない場合にメーカーに違約金を課す契約条項）を課する場合，どの時点において要求事項に対する達成判断を行うか，双方にとって重要となる。

ユーザーとメーカー間では，判断時期をあらかじめ取り決めるため，メーカーでは，製品リリース後の故障発生状況を把握して今後の推移を予測する。

もし未達成が予測される場合には，何らかの不具合等のリスクが顕在化する可能性が疑われることや，ペナルティの回避のため，早期に原因究明，対策を行うことが重要となっている。Erlang法などの数学的な予測計算手法が活用されている。

このようにRAMSでは，製品リリース後も含めた製品製造から，営業，改修，使用終了まで含む製品ライフサイクル全体を通した活動が計画されていることにより，営業段階においてなお，リスクベースでのアプローチが製品に対して継続される。

前述のようにユーザーの機微情報にも関わるため，メーカーが把握できる範囲は限られることも多いが，可能な限りリスクを把握し，対策を行うことで製品の品質向上に努める仕組みでもある。

7. まとめ

本稿では鉄道に関する機能安全規格「RAMS」の概要と，RAMSを通じて，機能安全による安全性を保つための手法とリスクベースの考え方を紹介した。

RAMSに基づく製品開発手順のうち，故障の種類や品質管理が重視されている点など，特徴的な考え方を述べ，RAM及びSafetyの各要素に対する目標設定，部品への目標割り当て手順などのメーカー・インテグレーターが行う業務の例と，コストを意識しRAM各要素の調整を行うイメージも紹介した。

また，ユーザーが行う，フィールドデータによるRAMS要素の分析活動の必要性を述べた。

最後に，日本国内では，何も言われなくとも迅速で丁寧なアフターセールスに努めており，文化ともいえる。一方RAMS等の機能安全では，計画等の管理がない状態は，無秩序で，リスクのある状態と考える。しかし，RAMS等の機能安全は，なかなかうかがい知れない製品品質，安全性，顧客重視の取り組みも，活用の仕方次第で実証するツールとなるものと考えている。

本稿が，技術進展の進む船舶分野において，何かのご参考，ご検討の一助となりましたら幸いです。

参考文献

1) 厚生労働省：機能安全による機械等の安全確保について，https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/0000140176.html，（2023年8月15日閲覧）
2) 佐藤吉信：機能安全に関わる人材育成セミナー【基本領域】機能安全，一般財団法人日本規格協会，2013年9月，pp24
3) 福田隆文：IEC 62061　機械の機能安全規格の概要，安全工学2009年48巻6号，pp379-384
4) 田村兼吉：海事分野におけるリスクアセスメントについてーリスクとうまく付き合うー，ClassNK技報　No.6 2022(Ⅱ)，pp4
5) Rome Laboratory Air Force Material Command(AFMC), Reliability Engineer's Toolkit, pp90