


ソフトウェア工学


第6回: クリティカルシステム



2023年11月13日

星野 寛

Hiroshi Hoshino

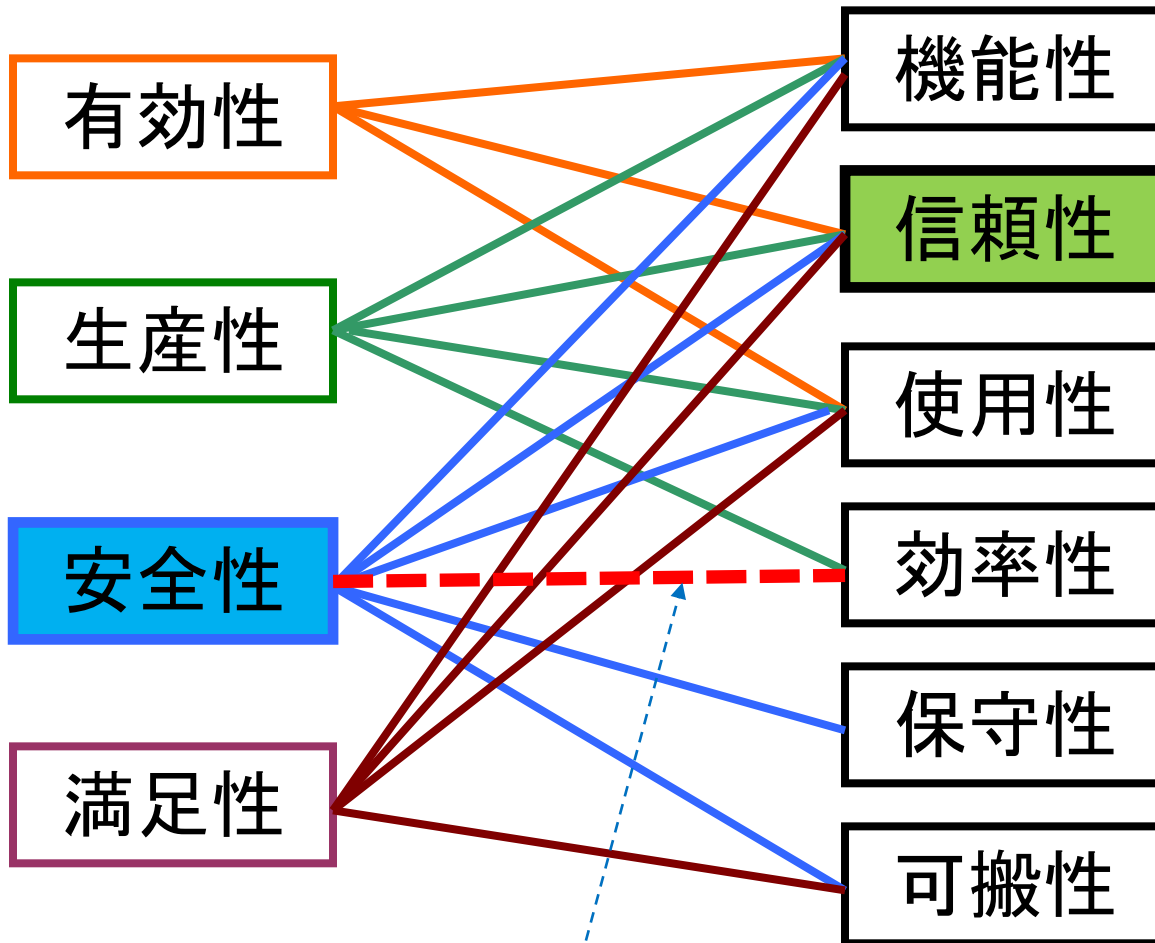


クリティカルシステム

品質特性間の関係

利用時
【ユーザ目線】

製品(規格)
【開発者目線】



相反することのように見える

信頼性と安全性

■ 広義の信頼性

- 信頼性(reliability)+保守性(maintenability)+...
- システムに対してユーザが信頼できる度合い. つまり, システムがユーザの意図通りに機能し, 普通の使い方をしていればおかしくならないだろうと, 信用できる度合い.

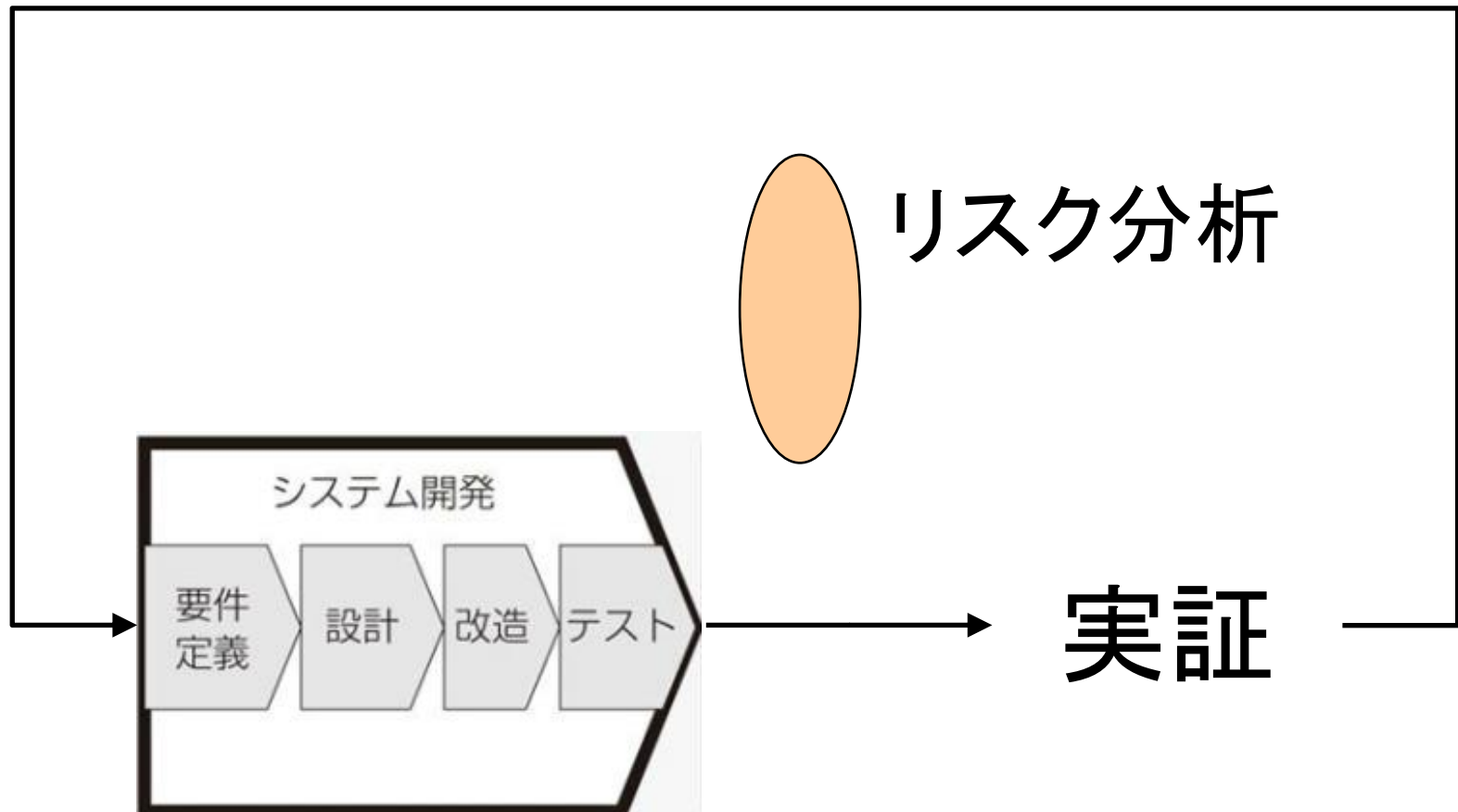
■ クリティカルシステムにとって最も重要な性質


- クリティカルシステム:障害により重大な人的・経済的結果を招く可能性をもつシステム
- クリティカルシステムでは, 障害によるコスト損失が大きいため, 信頼性を確保するために開発コストが「高い」開発方法論を適用**できる**

クリティカルシステムの例

- 安全性にクリティカルなシステム
 - 障害が生命・環境への被害・損害を与えかねないシステム
- 目的・使命にクリティカルなシステム
 - 障害により目的達成ができなくなるようなシステム
- 経済的にクリティカルなシステム
 - 障害による経済的・金銭的な損害が大きいシステム

クリティカルシステムの設計





自動運転システムの例

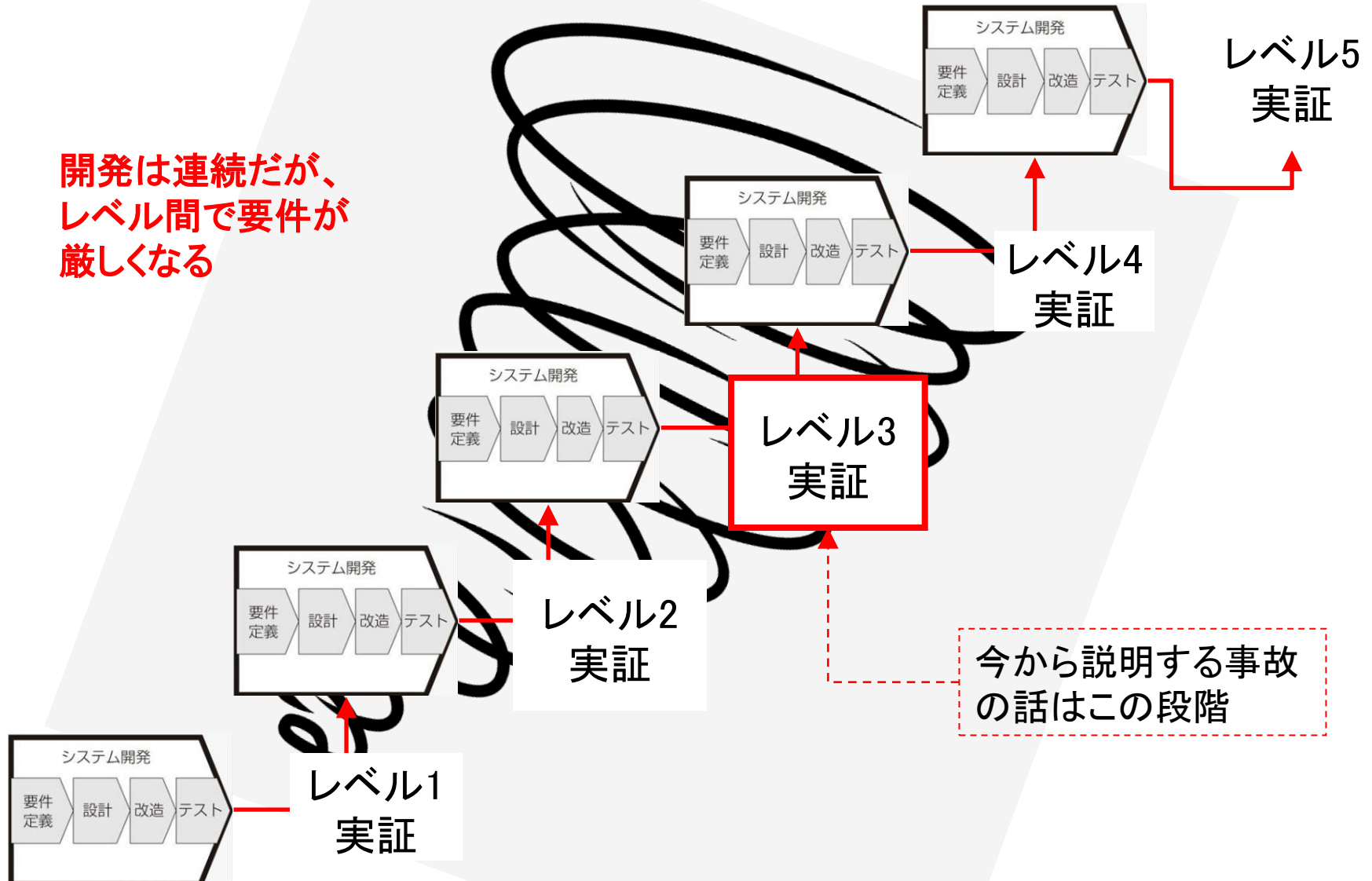
自動運転を例にしたリスク分析

自動運転化レベル

レベル	概要	運転操作の主体
レベル0	ドライバーが全ての運転操作を実行。	ドライバー
運転自動化なし		
レベル1	システムがアクセル・ブレーキ操作またはハンドル操作のどちらかを部分的に行う。	ドライバー
運転支援		
レベル2	システムがアクセル・ブレーキ操作またはハンドル操作の両方を部分的に行う。	ドライバー
部分運転自動化		
レベル3	決められた条件下で、全ての運転操作を自動化。ただし運転自動化システム作動中も、システムからの要請でドライバーはいつでも運転に戻れなければならない。	システム (システム非作動の場合はドライバー)
条件付運転自動化		
レベル4	決められた条件下で、全ての運転操作を自動化。	システム (システム非作動の場合はドライバー)
高度運転自動化		
レベル5	条件なく、全ての運転操作を自動化。	システム
完全運転自動化		

レベル上昇がスパイラルになる

開発は連続だが、
レベル間で要件が
厳しくなる



ウーバーの事故

- 2018年3月18日、ウーバーは自動運転レベル3の実証実験中に人身事故を起こした。
- (事故の映像:
<https://www.youtube.com/watch?v=06upo5tOGuQ>
)
- 当初、この事故はセーフティドライバが動画を視聴していたことが原因とされていたが、米国家運輸安全委員会(NTSB)は、2019年11月5日この事故に関する調査報告書を公表し、自動運転システムの設計に欠陥があったことを指摘した。
- 本講義では、システムの要求・設計段階でどのような考察・判断がなされたのかを推察しながら、「欠陥」をあらかじめ回避することはできなかったか考察する。

NTSB報告書

■ システム上の問題はおもに以下の3つ

1. 自動運転車のADSが被害者を歩行者と認識できなかった。
 - 自動運転車は事故発生時に時速約70キロメートルで走行していた。ADSのセンサーは衝突事故の5.6秒前に被害者の存在を検出したが、そのときは「車両」と認識していた。5.2秒前には「その他」と認識し、4.2秒前に再び「車両」とした。その後「車両」と「その他」で修正を何度か繰り返し、2.6秒前に「自転車」と認識した。その後も「不明」と「自転車」を行き来した。現実には自転車を押した歩行者だったが、最後まで「歩行者」とは認識できなかった。
 - 自動運転車は道路の右車線を走行し、被害者は車両の進行方向左側から右側に向かって道路を横切っていた。被害者は動いていたが、ADSは検出した対象が「静止している」と何度か予測していた。被害者が完全に車両の進路上にいるとシステムが予測したのは事故のわずか1.2秒前だった。その時に初めて衝突が差し迫っている危険な状況だとシステムが認識した。

NTSB報告書(続き)

2. ADSはその時、「動作抑制モード」に入った。

- ウーバーのADSは緊急事態を察知すると1秒間の動作抑制モードに入り、自動ブレーキの発動やドライバーへの警告を抑制した。ADSはその間に危険の詳細を再確認して代替経路を算出する設計だった。
- ウーバー側はこのモードの導入意図について、「開発中のADSが現実には存在しない危険な状況を誤って発見することで、車両に不要で極端な操作をさせるのを懸念したため」と説明している。つまりADSによる誤認識を考慮して、障害物を検出しても即座に自動ブレーキを作動させないようにしていた。
- 今回の事故では1秒間の動作抑制モードが終了しても、衝突の危険性は回避できていなかった。そこで衝突の0.2秒前にADSはドライバーに警報を鳴らし、自動的に減速し始めた。ドライバーがハンドルを操作した結果、ADSによる自動運転は終わり、ドライバーによる運転に切り替わった。しかし3月18日午後9時58分、衝突は起こった。ドライバーがブレーキを踏んだのは衝突の0.7秒後だった。

NTSB報告書(続き)

3. ウーバーの自動運転車はスウェーデンのボルボ・カーの多目的スポーツ車「XC90」にADSを取り付けたもの。
- 車両には工場出荷の段階でボルボの先進運転支援システム(ADAS)が搭載されていて、信進行方向に障害物があったら即座に警告音を鳴らしたり、自動的に急ブレーキが作動したりする仕様だった。しかし事故時点でボルボ製のADASはオフになっていた。
 - ボルボのADASとウーバーのADSはそれぞれ障害物検出レーダーを搭載していたが、どちらも同じ周波数を使っていたため、ADASとADSを同時に動かすのが難しかった。ADASとADSのどちらのブレーキ操作を優先させるのか、ブレーキシステム側での対応ができていなかったという事情もあった。これらの理由からADASとADSの併用は見送られた。

NTSB報告書(続き)

4. 運転者はスマホでフールー視聴。

- システムに関連するこれら3つの問題に加えて、安全確保の最後のとりでとなるべきセーフティードライバーも役割を果たせなかった。ドライバーは運転中に私物のスマートフォンで動画配信サービスの「フールー(Hulu)」を視聴していたと指摘されている。
- 自動運転車にドライバーが乗り込んでから衝突するまでの車内の様子は録画されており、ドライバーが頻繁にセンターコンソール周辺に視線を落としていた様子が記録されていた。午後9時31分から58分までの27分間に、204回は同じ場所を見ていた。
- ドライバーは自動運転車が走行状態にあった21分48秒のうち32%に当たる6分47秒間、道路に視線を向けていなかった。ドライバーはスマホをバッグの中に入れていたと主張している。しかし当局がフールーから入手した情報によると午後9時16分から59分までの間、ドライバーのアカウントに動画の視聴履歴があった。

NTSB報告書(まとめ)

1) 自動運転車のADSが被害者を歩行者と認識できなかった

対象の分類が数回にわたって変化したため、ADS(Automated Driving System)は対象の進路も正確に予測できなかった

2) 自動ブレーキを抑制していた

開発中のADSが現実には存在しない危険な状況を誤って発見することで、車両に不要で極端な操作をさせるのを懸念したため、1秒間の動作抑制モードに入り、その後対象物の再認識を行うこととしていた

3) ボルボ製のADASはオフになっていた

ボルボのADASとウーバーのADSはそれぞれ障害物検出レーダーを搭載していたが、どちらも同じ周波数を使っていたため、ADASとADSを同時に動かすのが難しかった。

4) 運転者はスマホで動画を視聴

衝突の0.2秒前に警報で車内のテストドライバーに危険を知らせたが、ドライバーは動画を視聴していて前方から目を離していた。

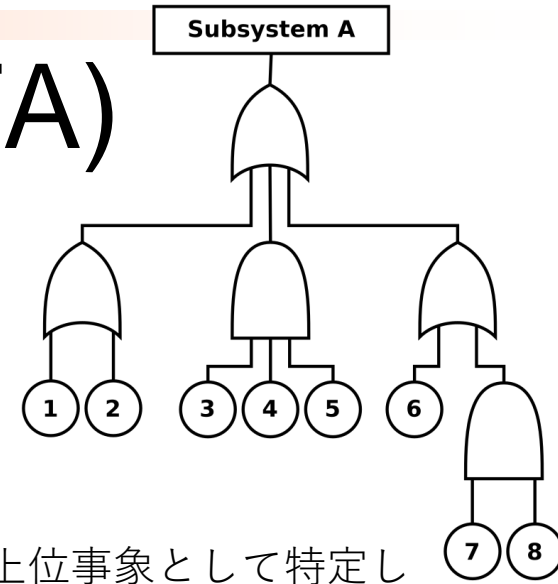
- NTSBは2019年11月19日、ドライバーの不注意が事故の直接の原因ではあるが、ウーバーの安全文化が不十分であったことも事故の原因となったとの判断を下したと発表している。



リスク分析ツールの例

フォールトツリー解析(FTA)

- 故障・事故の分析手法。
- 故障木解析ということもある。
- FTAの実行



1. 解析対象（システム）を明確にする

- 望ましくないイベント（不具合、故障、事故など）を上位事象として特定します。

2. 要因を見つける

- 上位事象の発生につながる可能性のある要因事象を系統的に、漏れや重複がないよう抽出し、列挙します。

3. FT図の作成に取りかかる

- 論理記号とコネクターを使い、上位事象と要因事象を論理的に接続します。上位事象、他の事象（中間事象）、基本事象をトップからボトムまで配置します。






4. フォルトツリーの定量解析を行う

- 基本事象の発生確率を「非常に高い」「高い」「低い」などのレベルで分析し、さらに下位事象の発生確率とその因果関係から上位事象の発生確率を求めます。

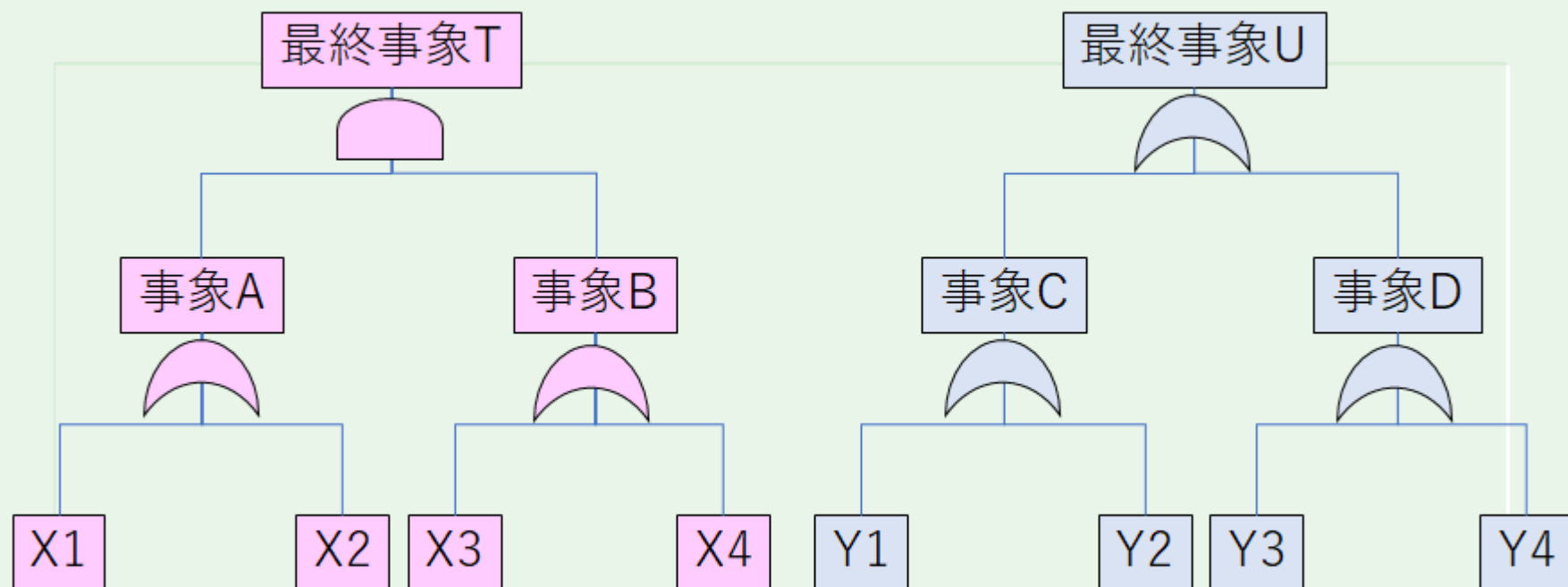
5. 対策を検討して改善する

- 原因を見つけることは最終的な目標ではありません。FTAを行う目的は、実際に問題を解決して障害を取り除くことです。ブレインストーミングを行い、それぞれの重大障害の根本原因に対処する行動、解決策を検討し、故障や不具合を改善します。

FTAに用いられる記号

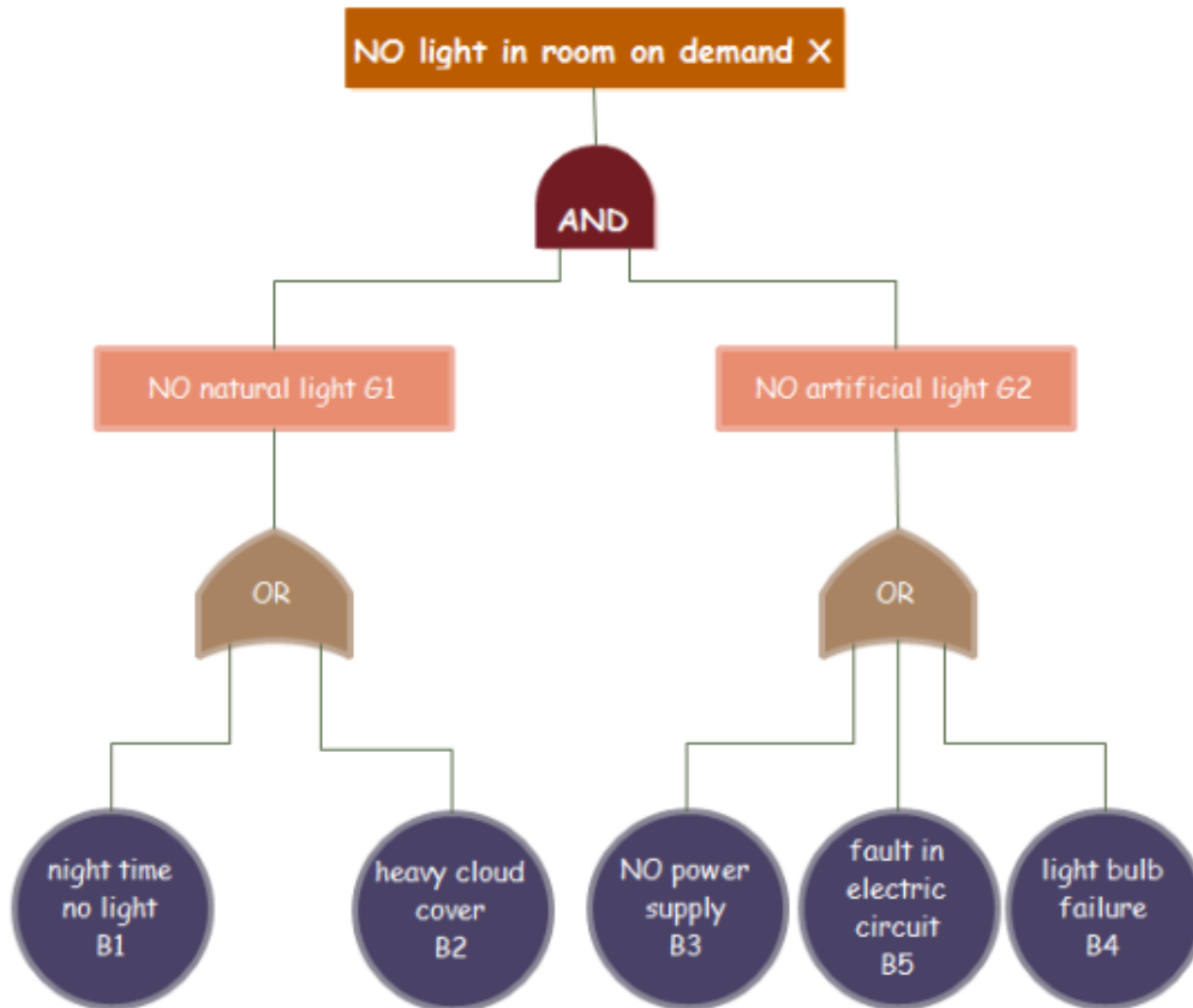
記号	名称	説明
	事象	故障、不具合などの現象
	基本事象	これ以上要因系を考えない事象
	AND	下位事象が同時に発生するとき、上位事象が発生する
	OR	下位事象のうちどれか一つが発生するとき、上位事象が発生する
	非展開事象	情報・技術の未熟のため、これ以上は展開しない事象

最終事象の確率計算方法

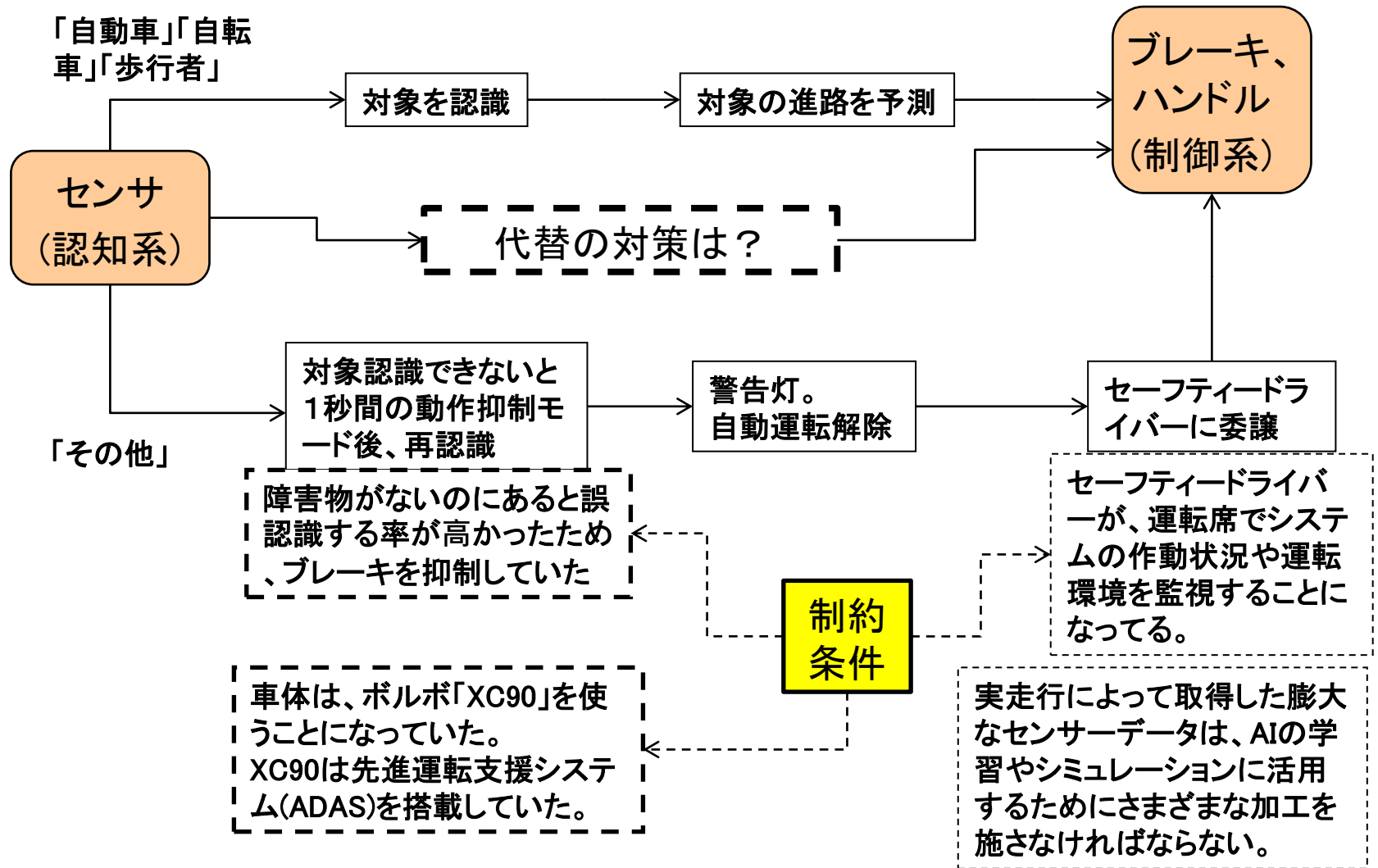


$$T = A \times B = (X1 + X2) \times (X3 + X4) \quad U = C + D = (Y1 + Y2 + Y3 + Y4)$$

FTAの例：部屋が暗い



ウーバー自動運転制御



ウーバー事故の事象と理由

回避できなかった理由

道路を横切る歩行者を認識できなかった

対象の進路も正確に予測できなかった

前方に障害物を発見しても、1秒間は自動ブレーキが動作しない設定であった(動作抑制モード)

セーフティドライバーが、運転席でシステムの作動状況や運転環境を監視することになっており、問題が発生した際にはドライバーがハンドルやアクセル、ブレーキを直接操作したり、センターコンソールにある赤いノブを押し倒したりする。そうするとADSからドライバーに運転が切り替わる

自動運転車(ボルボ「XC90」)の先進運転支援システムは**オフ**になっていた

ブレーキが遅れた理由

自動運転システム(ADS)のセンサーは衝突の約6秒前に被害者を検出していたが、ADSはそれが歩行者だと認識できなかった。交通ルールを無視した歩行者や自転車に乗った人だと正確に予測できていなかった。被害者は横断歩道ではない場所を横切っており、ADSは設計上、交通ルールを無視する歩行者を想定していなかった

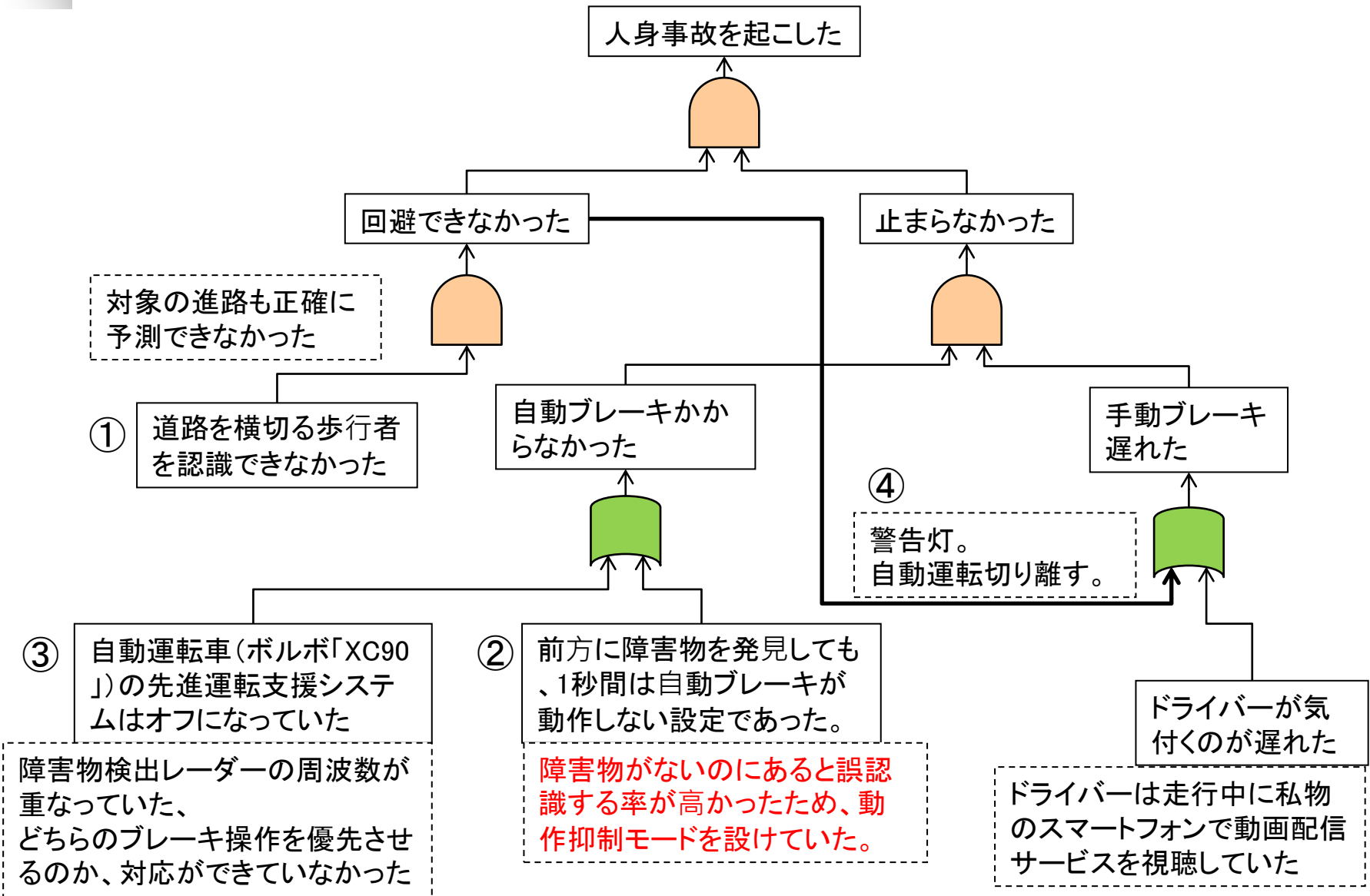
障害物がないの**にあると誤認識する率が高かった**ため、ブレーキを抑制していた。ADSはその間に危険の詳細を再確認して代替経路を算出する設計だった。

今回の事故では1秒間の動作抑制モードが終了しても、衝突の危険性は回避できていなかった。そこで衝突の0.2秒前にADSはドライバーに警報を鳴らし、自動的に減速し始めた。ドライバーがハンドルを操作した結果、ADSによる自動運転は終わり、ドライバーによる運転に切り替わった。しかし3月18日午後9時58分、衝突は起こった。ドライバーがブレーキを踏んだのは衝突の0.7秒後だった。

ドライバーは走行中に私物のスマートフォンで米動画配信サービスを視聴していた

ウーバーの自動運転システムによる自動運転中は、ボルボの先進運転支援システムは作動しなくなるように設計されていた。(障害物検出レーダーの周波数が重なっていた、どちらのブレーキ操作を優先させるのか、ブレーキシステム側での対応ができていなかった))

ウーバー自動運転事故のFTA



背景

- 開発競争が激しく、開発期限があった
 - 短期間で改良が必要
 - ドキュメントとコードが乖離？
- 過去の実験で、対象の認識が不安定であった
 - サンフランシスコでの実験⇒信号無視
 - 改良結果がドキュメントに反映されなかった？
 - 対象を認識できなければ対処できない⇒対象認識の改良のみ？
- 過去の実験で、よく停止していた（「自動運転タクシー」のイメージダウン）
 - 「止めない」が最大要件となった？
- 基本車体として、ADAS機能を持つボルボ社「XC90 SUV」を使うことになった（提携）
 - 開発中のシステムを過信していた？
 - ADAS無しでもレベル3では安全？

ウーバー自動運転事故後改善

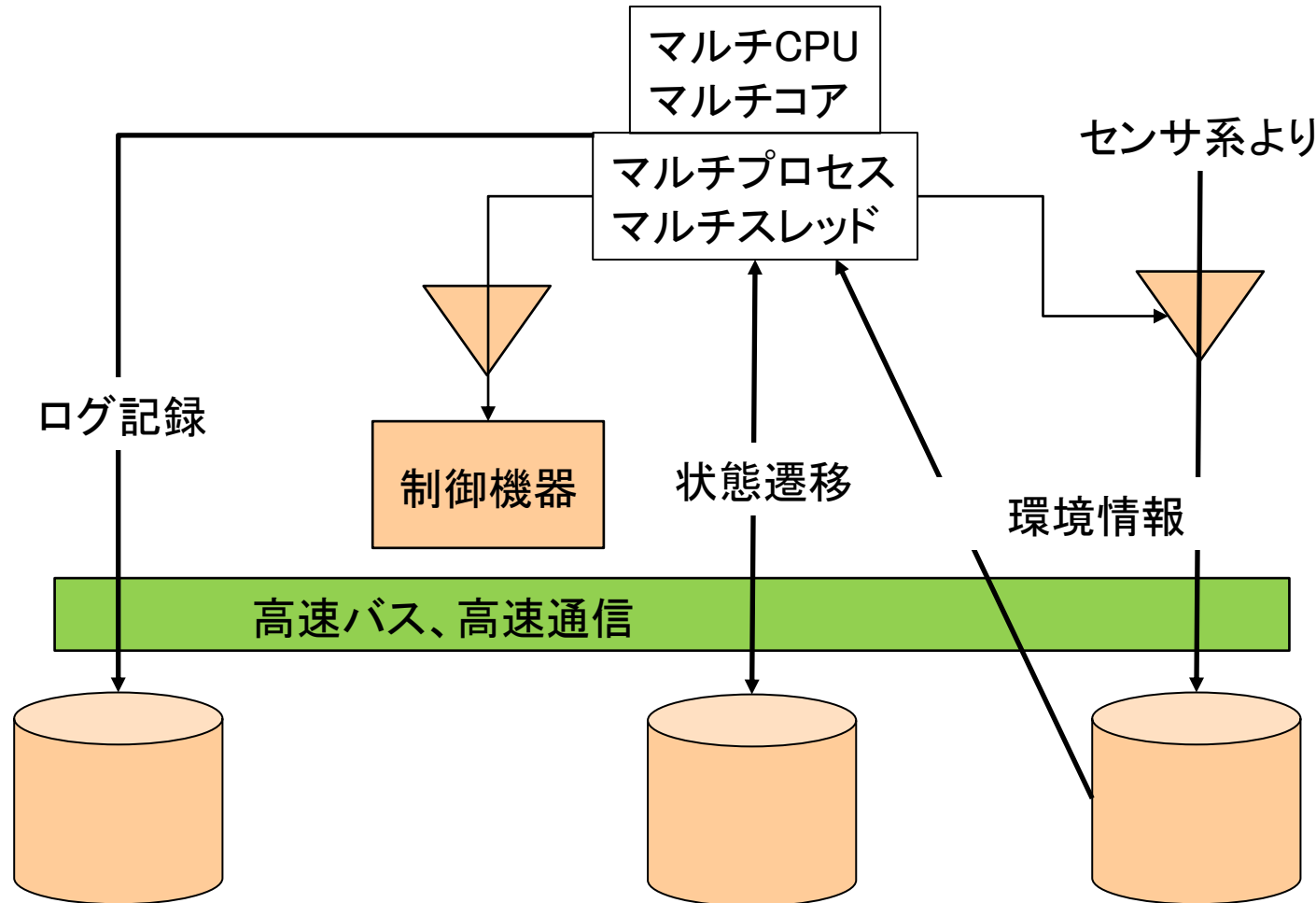
- センサーが検出した対象の進路を予測するアルゴリズムを修正した。
 - ①対象の分類が変わっても対象の以前の位置からその進路を予測できるようにした。
 - 同じ条件でも衝突の4.5秒前に歩行者を正確に発見し、分類できるだろうと報告している。
- ②緊急時における1秒間の動作抑制モードは廃止した。
 - ④ブレーキをかけても手遅れであるような場合であっても、衝突の勢いを軽減するためにブレーキを作動させるように改めた。
- ③ボルボのADASが備える歩行者を対象とした自動ブレーキ機能は、自動走行中でも作動するようにした。

事故後改善を設計時に気づく？

- レベル 2 での改善で、仕様の正当性を過信した？
 - レベル 2 からレベル 3 へは、要件が変わったが、再レビューが手薄？
- 実際には、仕様書とコードは乖離していた可能性大
 - 真っ白な状態から要件定義、設計をしている余裕はなかった
 - レベル 2 の仕様書がFIXしていたか？
- 設計変更は、開発工数に影響
 - 対象物の認識とその行動予測だけでなく、並行して物体の移動ベクトルの分析が必須
 - ボルボのADASとの共存は、ハードの変更も加わる
- ⇒でも、プロなら気付くべし。

冗長、非同期並行処理

惜しまず、開発コストが「高い」開発環境



設計・レビューはチームプレー：情報共有、意識共有