University of Tsukuba
筑波大学

日本機械学会２０１７年度年次大会
２０１７年９月５日
埼玉大学

自動運転のヒューマンファクター

筑波大学副学長・理事
稲垣　敏之

inagaki.toshiyuki.gb@u.tsukuba.ac.jp
http://www.css.risk.tsukuba.ac.jp

航空機における自動化の進展

1900年代初頭は、操縦の困難さをパイロットの練度で克服

- パイロットの負担が大
- ヒューマンエラーが入り込む余地

解決策のひとつは、人が担当している機能の自動化

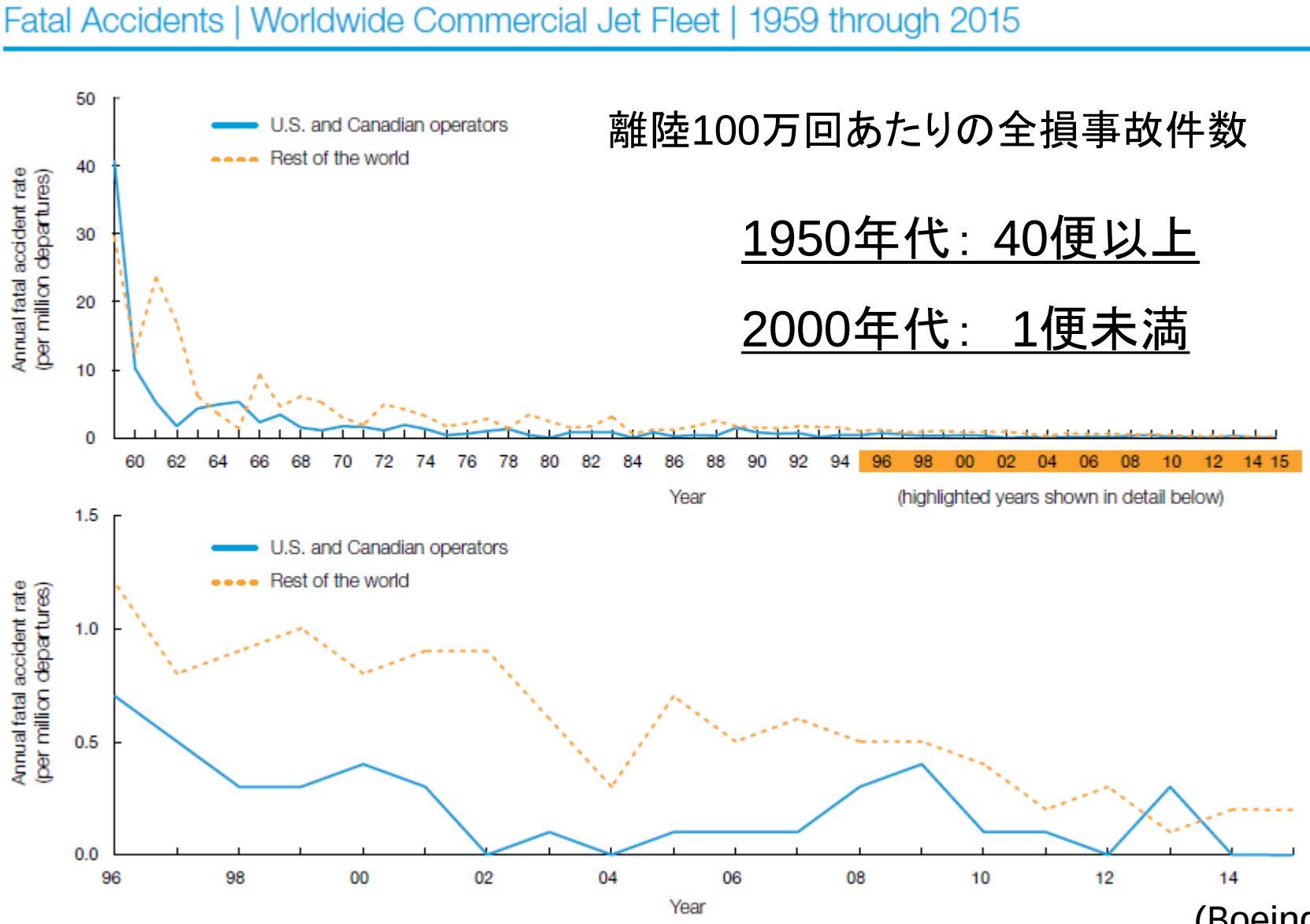
操縦操作の自動化だけでなく、飛行管理（機体重量や気象条件に合った離陸速度・上昇速度・巡航高度・降下開始点等の決定）も自動化

- 長距離路線を担当しているパイロットの年間飛行時間が800–900 時間とすると、そのパイロットが自ら操縦を担当しているのは、3時間程度

・・・　自動化できていないのは離陸フェーズだけ

（稲垣 2012）

高い知能と自律性を備えた機械がもたらす光と影（1）



離陸100万回あたりの全損事故件数

1950年代：40便以上

2000年代：　1便未満

(Boeing 2016)

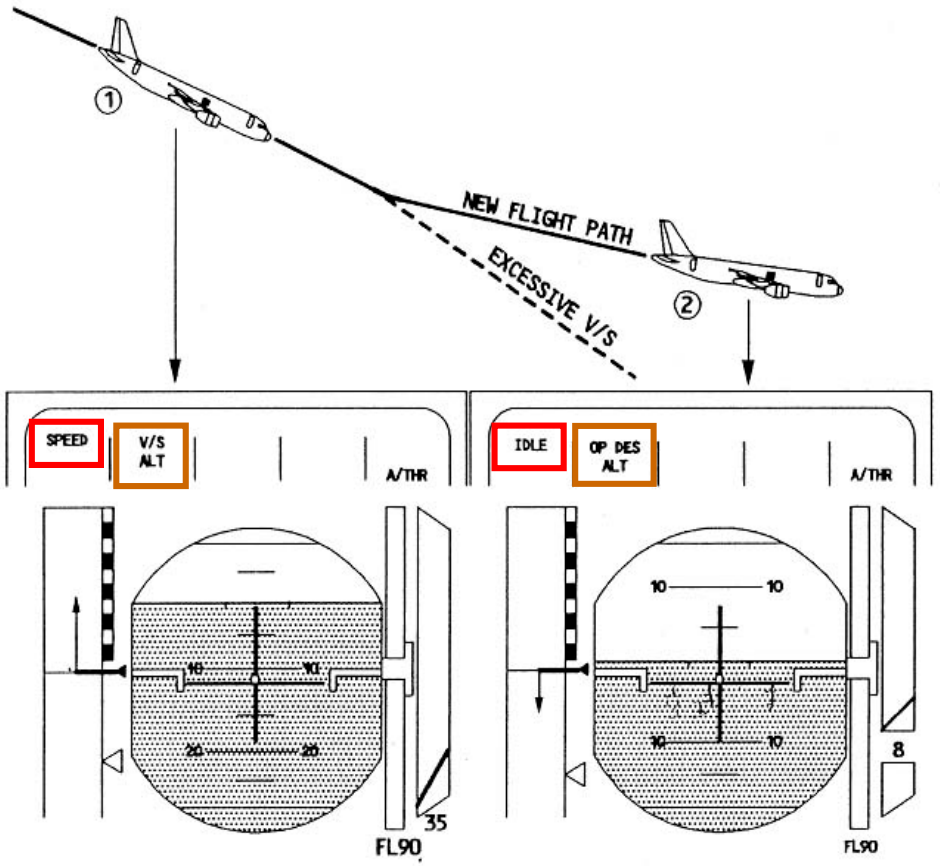
高い知能と自律性を備えた機械がもたらす光と影(2)

賢い機械

- 状況センシング
- 状況理解
- 何をなすべきかを決定し、実行

→ 状況認識の喪失
→ 機械への過信と不信の交錯
→ オートメーションサプライズ

(Inagaki 2006; 稲垣 2012)



状況認識

レベル1: 何かが起こっていることに気づく

レベル2: その原因を特定できる

レベル3: これからの事態の推移が予測できる

「自動運転」といっても、その形態は多種多様

Photo: BMW

Photo: Volvo

Photo: Zoox

自動運転レベル (Levels of Driving Automation： LoDA)

ドライバーは動的運転タスクの一部を担当 （走行環境監視はドライバーの役目）		
1	Driver Assistance	システムは縦方向制御／横方向制御のいずれか一方を担当。 ドライバーは動的運転タスクの残余分すべてを担当。
2	Partial Driving Automation	システムは縦方向制御と横方向制御の両方を担当。 ドライバーは動的運転タスクの残余分すべてを担当。
システムは動的運転タスクのすべてを担当		
3	Conditional Driving Automation	システムは動的運転タスクのすべてを担当。ユーザーに運転交代を求めたいときは、時間余裕をもってユーザーに要請。 ユーザーは、システムの要請に適切に対応すること。
4	High Driving Automation	システムは動的運転タスクのすべてを担当。システム／車両の故障や想定作動環境からの逸脱等が発生しても、システムはユーザーの手助けを求めることなく適切に対応。
5	Full Driving Automation	あらゆる道路条件、走行環境条件下で、システムは動的運転タスクのすべてを担当。

(SAE 2016)

LoDA 2 – Partial Driving Automation

システム:　縦方向制御と横方向制御の両方を担当。
ドライバー: 走行環境監視を含め、動的運転タスク残余分を担当。

Photo: BMW

監視制御(supervisory control)

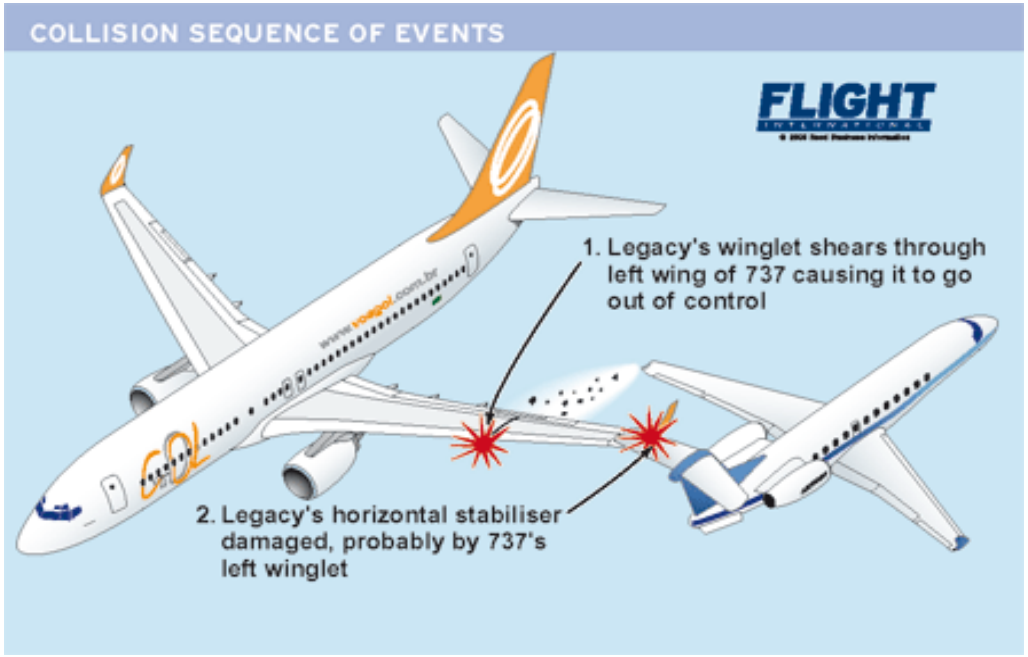
- 人が何をなすべきかを決め、システムに指示
- システムは、人の指示に沿って制御を実行
- システムによる制御の適切性を人が継続的に監視
- 人は、必要に応じてシステムが行っている制御に介入

システムの動作原理、能力限界、サブシステム間の相互干渉等に関する正確な理解が必要

← HMI のデザインが鍵

- ドライバーが監視制御をしていないと思えるときはどうする？

システムの作動／不作動が分かるか



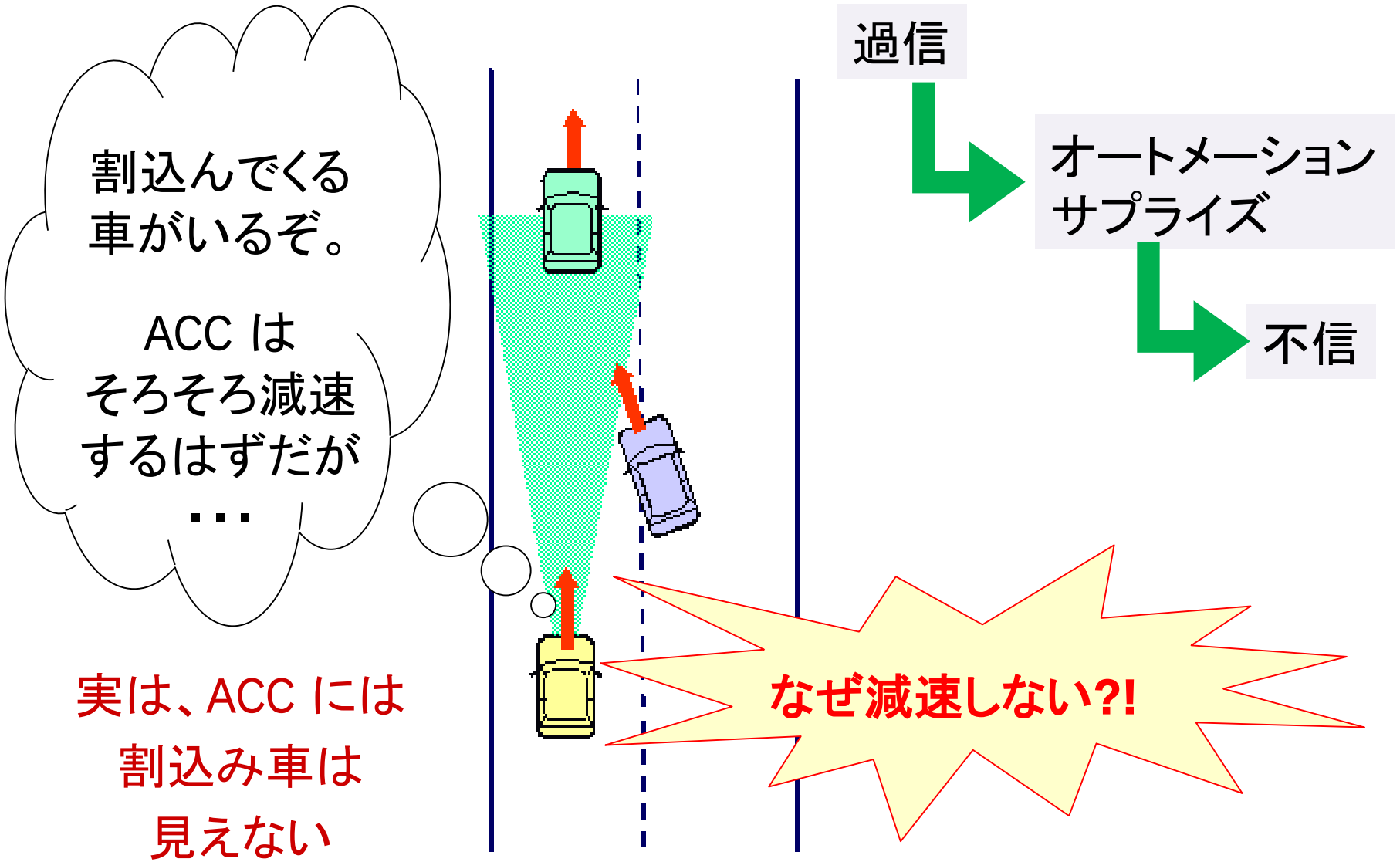
2006年9月、Boeing 737 と Embraer Legacy が アマゾン上空で衝突

(Flight International, 6 December 2008)

- Legacy のトランスポンダーは standby モード（送受信機能喪失）
- 「TCAS OFF」は表示されたが、目立たない白字表示
- Boeing 737 と Legacy に搭載されていた TCAS は、いずれも相手機の存在を知ることができない状態

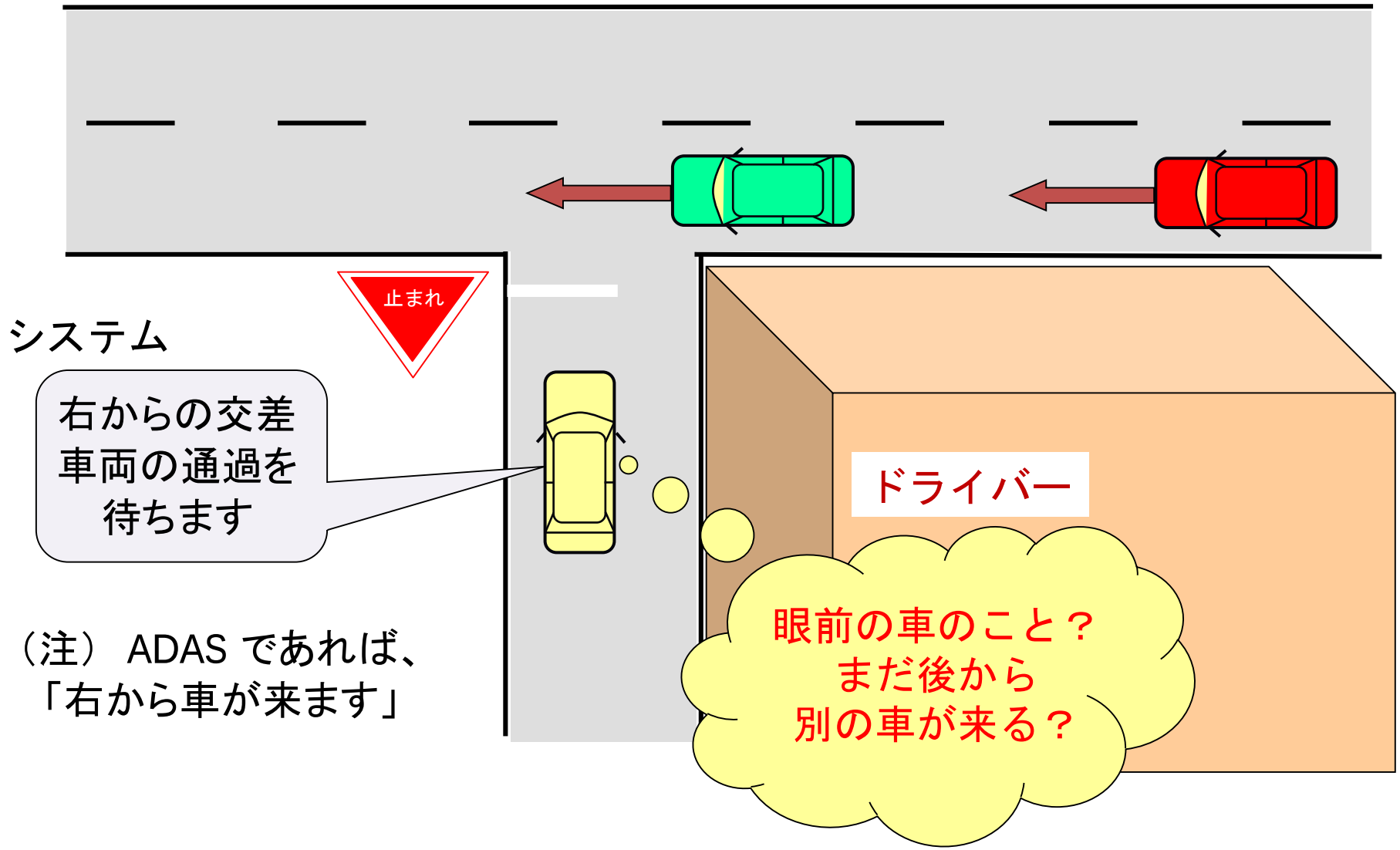
➡ TCAS 警報が発せられないまま、2機が衝突

システムの能力限界が把握できるか



（Inagaki 2010; 稲垣 2012)

システムと状況認識を共有できるか



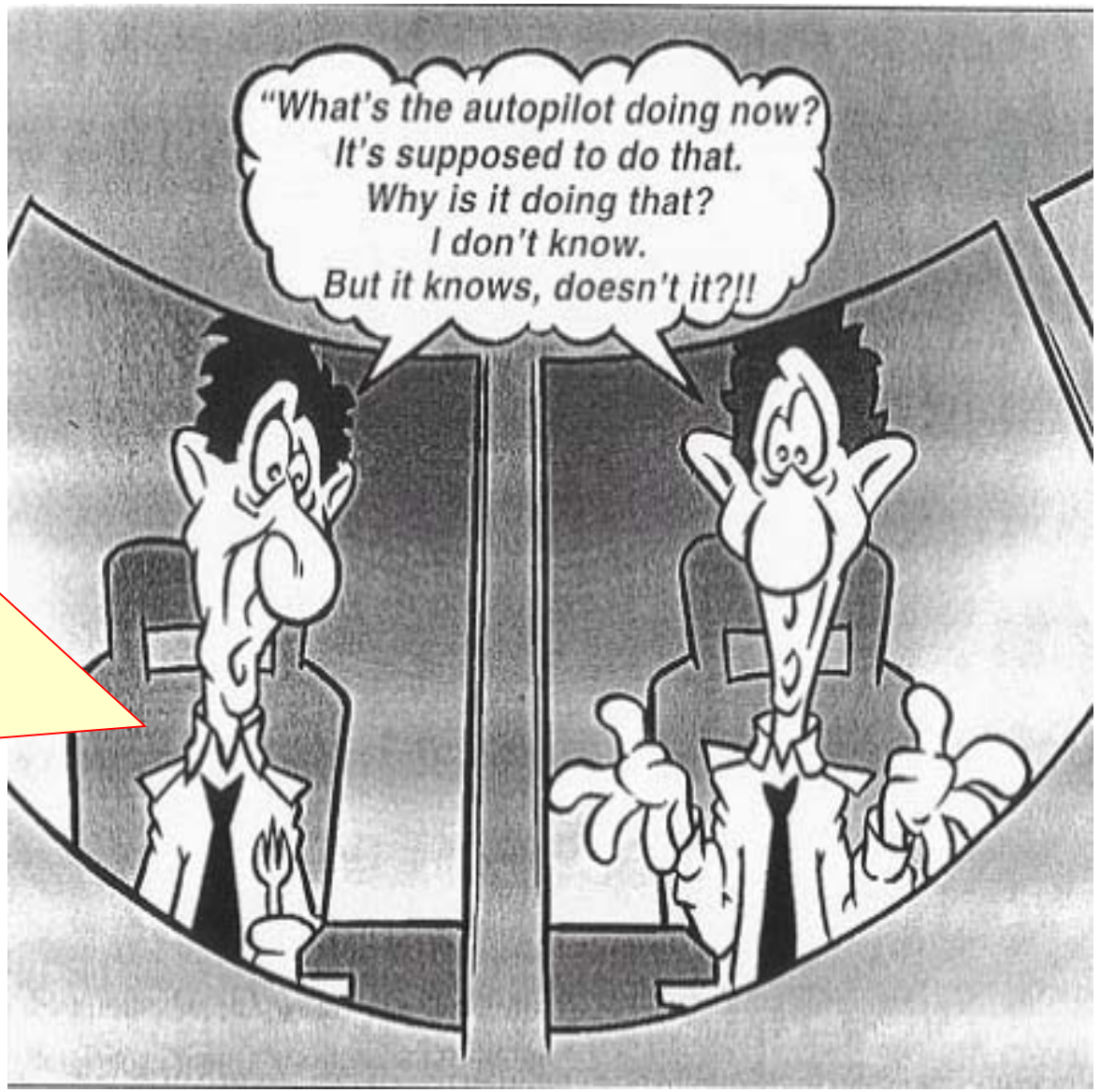
（注） ADAS であれば、
「右から車が来ます」

（Inagaki 2010; 稲垣 2012)

システムの意図の背景が分かるか？

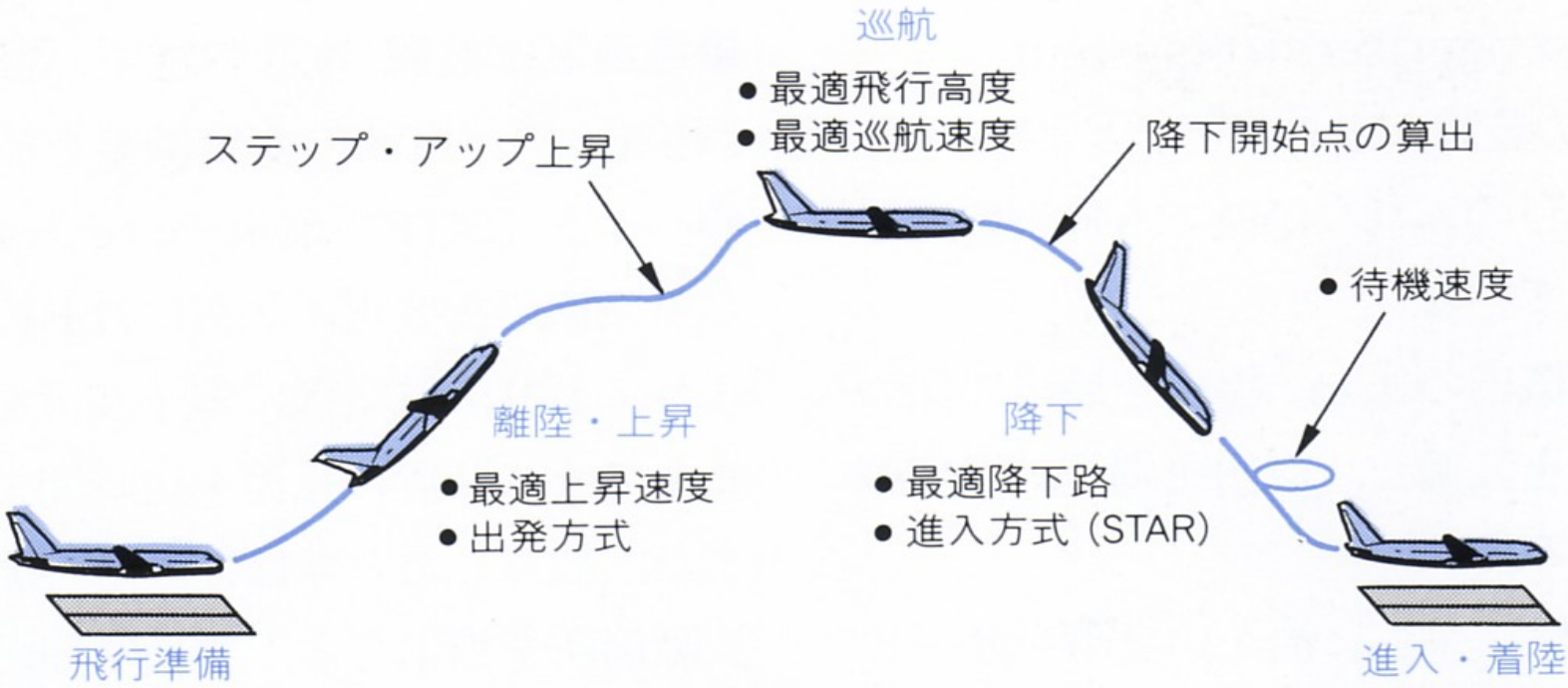
なぜ
オートパイロットが
こんなことをするのか
私にはわからない。

でも、
オートパイロットは
わかったうえで
やっているはず
だよね。



(FAA 1995)

航空機の自動化は LoDA 2 と同等



パイロットは安全運航の責を負い、システム状態と飛行環境を監視

➡ 定期的なシステム機能・原理等の教育、使用法の訓練を受ける

➡ クルマの自動運転のための教育・訓練や免許制度は？

LoDA 3 – Conditional Driving Automation

システム：　走行環境監視を含め、すべての動的運転タスクを担当。
ユーザーに運転交代を求めたいときは、十分な時間余裕をもって要請（Request to Intervene：RTI）を発出。

ユーザー：　RTI が発出されたときは適切に対応すること。

Photo: Volvo

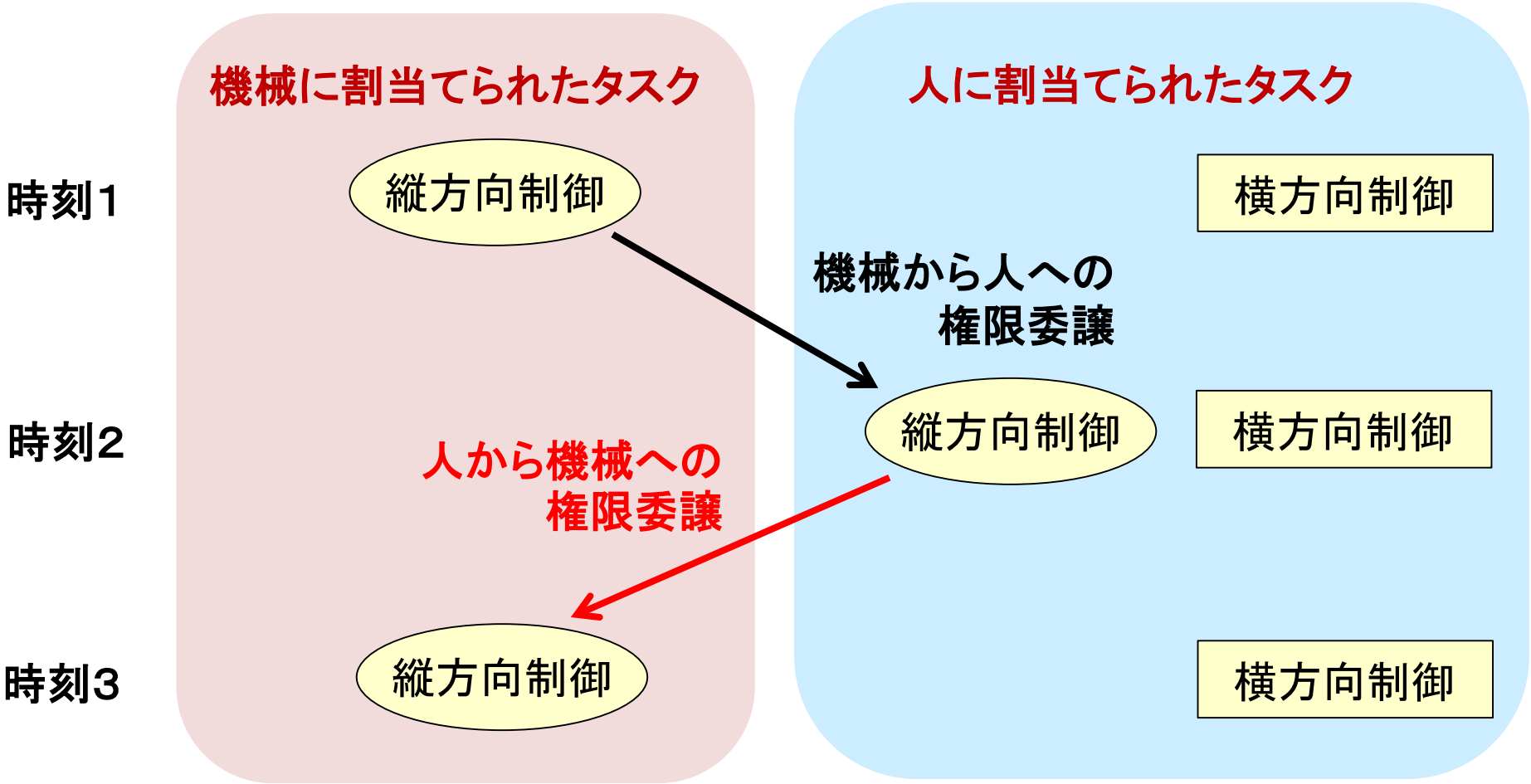
- 「十分な時間余裕」とはどれくらい？
- 運転交代を要請して一定時間経過後システムは機能停止してよい？
- レベル3の自動運転の狙いは何？

- 「システムの手に余るときは、人に対応してもらおう」という設計思想は妥当か？
- ユーザーは、結果予見義務／結果回避義務（過失責任）から解放されているのか？

運転主体の交代：　権限委譲（trading of authority）

（1）誰から誰への権限委譲？

（2）権限委譲の要否と実行タイミングを決定・実行するのは誰？

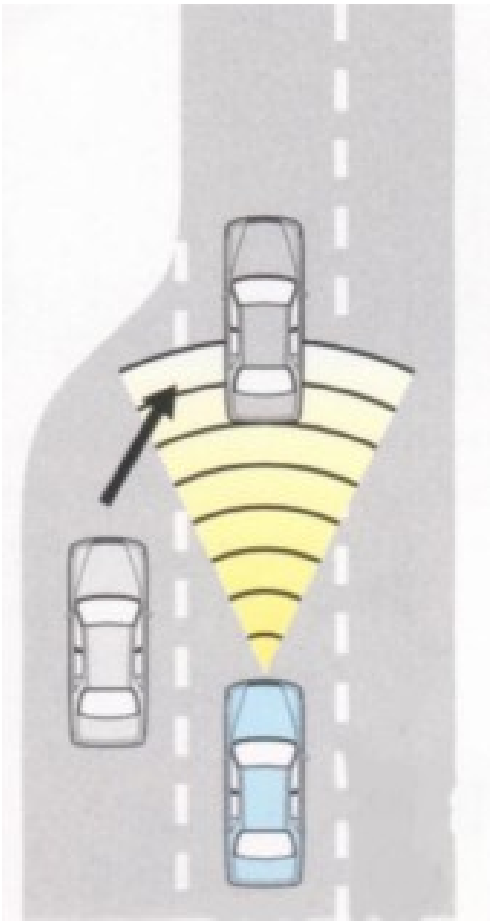


（Inagaki 2003; Inagaki & Sheridan 2012;　稲垣　2012）

人の判断による権限委譲

（例１） 離陸時は人間が操縦。
機体が安定すると、コンピュータに操縦を委任。
必要に応じてオートパイロットを解除して、
人が操縦。

（例２） ACC で走行中、割込みの気配を示す車に気づく。いったん ACC を解除し、割込み車との間隔を適切にした後、再び ACC をエンゲージ。



機械の判断による「機械から人への権限委譲」

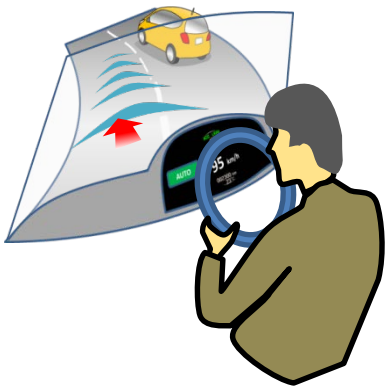
ユーザー：運転操作は行わず、走行環境の監視もしていない。
システムから運転交代を求められたとき、
瞬時に状況を見極め、適切に車両を制御する。

**10秒後に自動走行モードを解除します。
運転を交代してください**

120 km/h なら 333 m

60 km/h なら 167 m

システムから人へ
権限を円滑・安全に
移行させたい

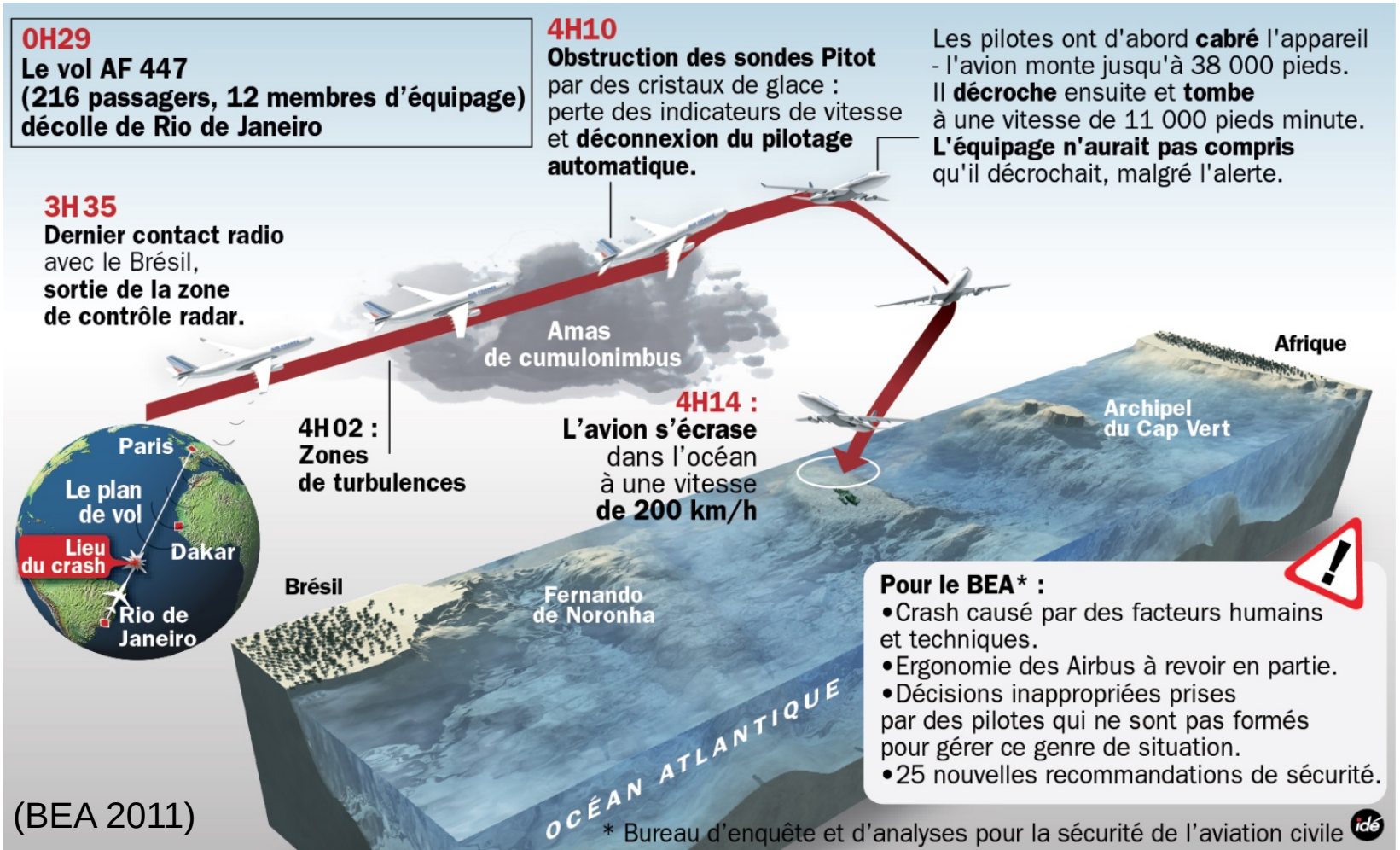


機械から人への権限委譲は成功するとは限らない

エールフランス447便（A330-200）の墜落（2009.06）

高高度を飛行中に対気速度に矛盾が生じ、オートパイロット解除。

その後のパイロットの操作が不適切であったため異常姿勢に陥り、墜落。



(BEA 2011)

自動化レベル (Levels of Automation: LoA)

レベル	定　義
1	システムの支援なしに、すべてを人が決定・実行。
2	システムはすべての選択肢を提示し、人はそのうちのひとつを選択して実行。
3	システムは可能な選択肢をすべて人に提示するとともに、ひとつを選んで提案。 それを実行するか否かは、人が決定。
4	システムは可能な選択肢の中からひとつを選び、それを人に提案。 それを実行するか否かは、 人が決定。
5	システムはひとつの案を人に提示。人が了承すれば、システムが実行。
6	システムはひとつの案を人に提示。 人が一定時間内に実行中止を指令しない限り、システムはその案を実行。
6.5	システムはひとつの案を人に提示すると同時に、その案を実行。
7	システムがすべてを行い、何を実行したか人に報告。
8	システムがすべてを決定・実行。人に問われれば、何を実行したかを報告。
9	システムがすべてを決定・実行。 何を実行したかを人に報告するのは、報告の必要性をシステムが認めたときのみ。
10	システムがすべてを決定し、実行。

人に最終決定権あり

機械に最終決定権あり

(Sheridan 1992; Inagaki et at. 1998)

自動化レベル1： ナイトビュー

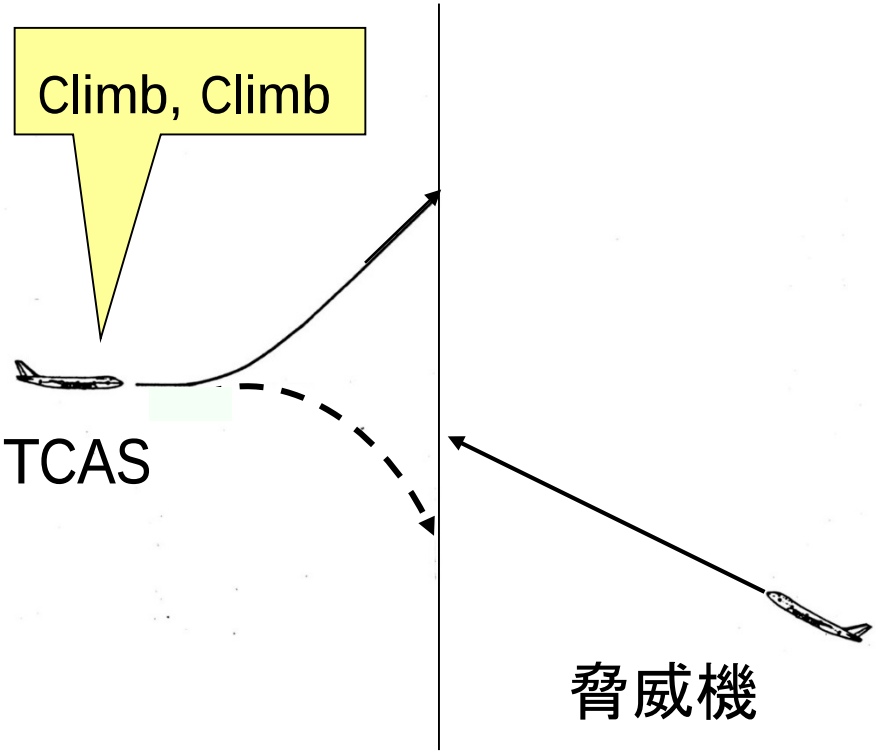
車載の暗視カメラで捕らえた前方映像を解析し，その中に歩行者が映っていることを検知したとき，歩行者に枠をつけてディスプレイに表示する （注意喚起）

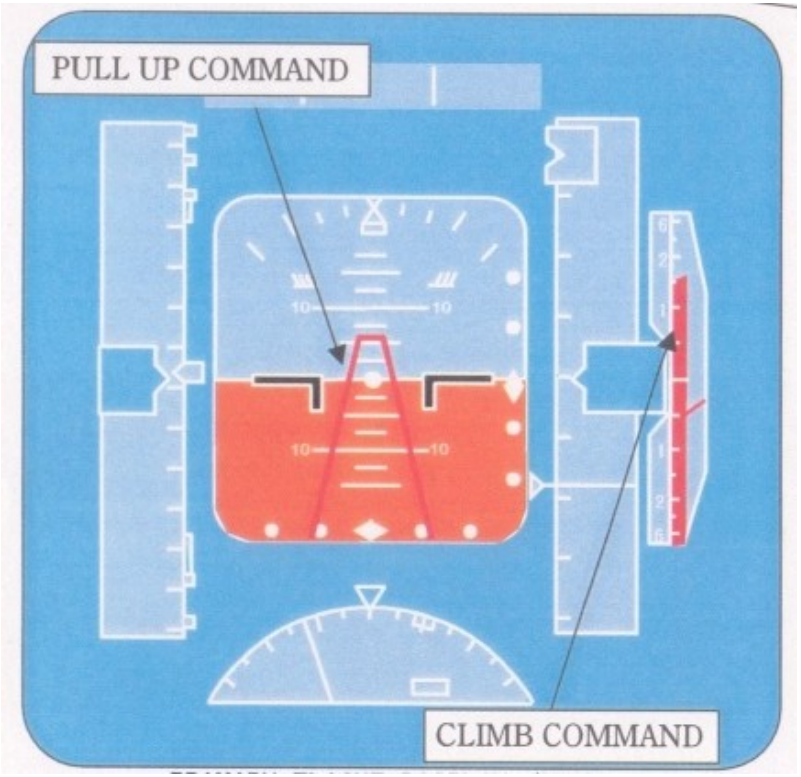
LoA 1　システムの支援なしに、すべてを人間が決定・実行

自動化レベル4： TCAS

LoA 4　システムは可能な選択肢のうちからひとつを選び、
それを人に提示。それを実行するか否かは人が決定

回避アドバイザリ

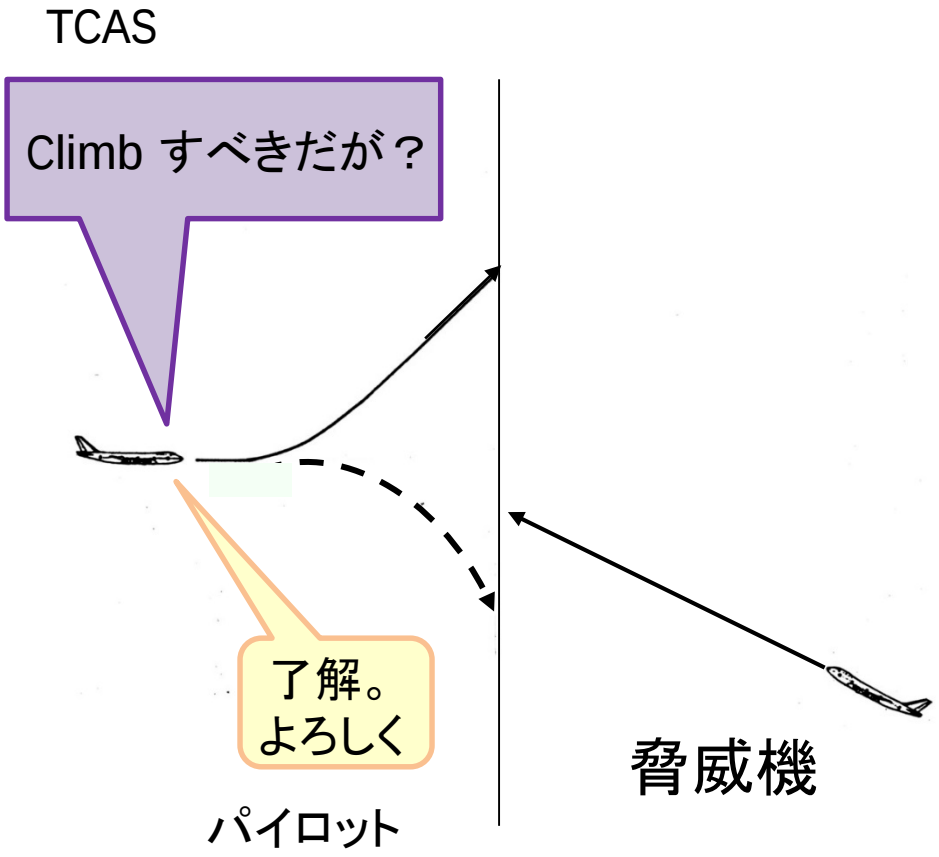


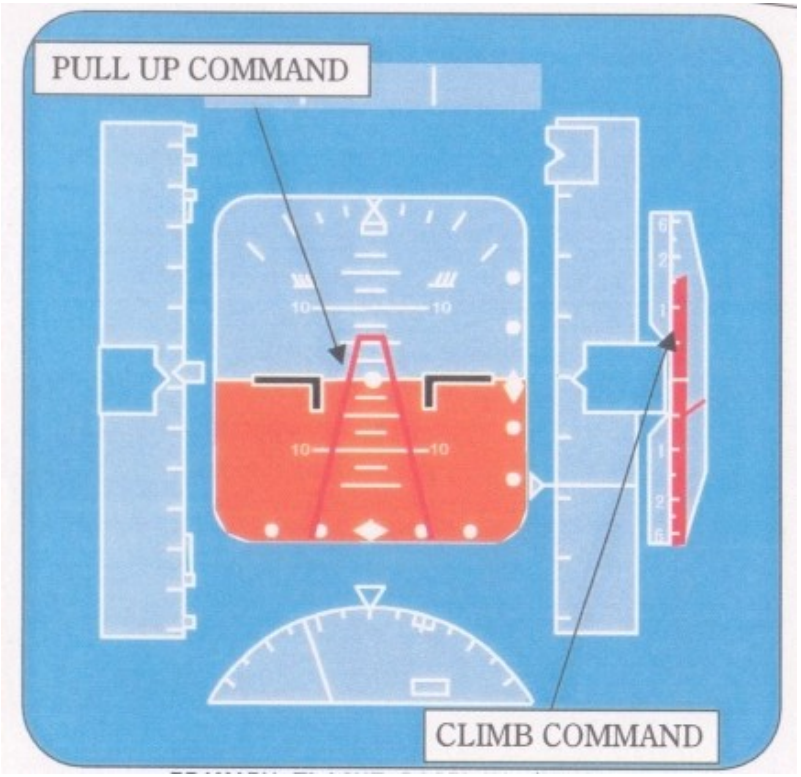


機械は助言をするが、場合によっては、人は助言を無視できる

自動化レベル5： TCAS（仮想的）

LoA 5　システムはひとつの案を人に提示。人が了承すれば、システムが実行





自動化レベル 6:　急減圧検知時の自動降下

LoA 6　システムはひとつの案を人に提示。
人が一定時間内に実行中止を指令しない限り、システムはその案を実行

① システムが客室急減圧を検知

② システムは乗員に告知し、同時に
緊急降下のカウントダウン開始

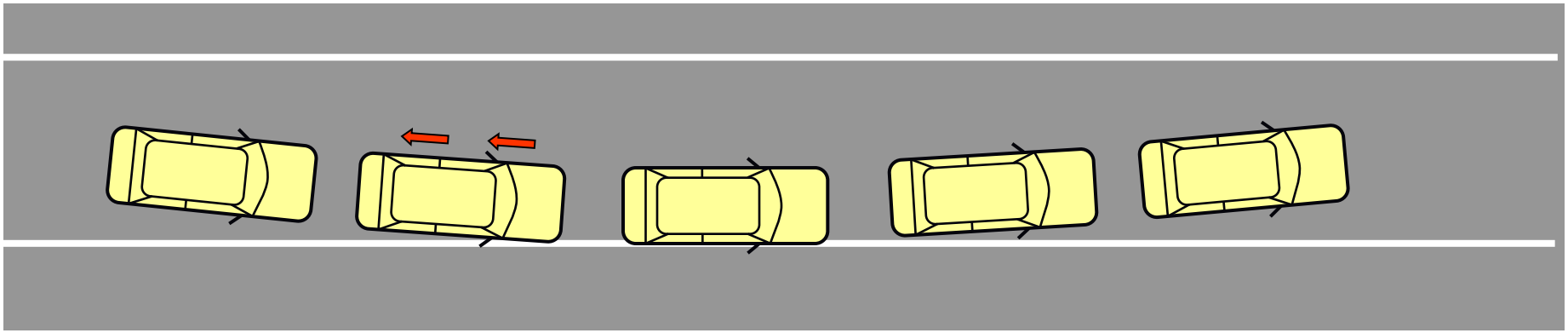
③ カウントダウン終了までに
乗員が拒否権を発動しなければ、
システムは緊急降下を実行

操作開始の遅れ

**機械が人に提案を行ったとき、限られた時間内に人が
明確な拒否を表明しない限り、機械はその提案を実行**

自動化レベル 6.5： 車線逸脱防止システム

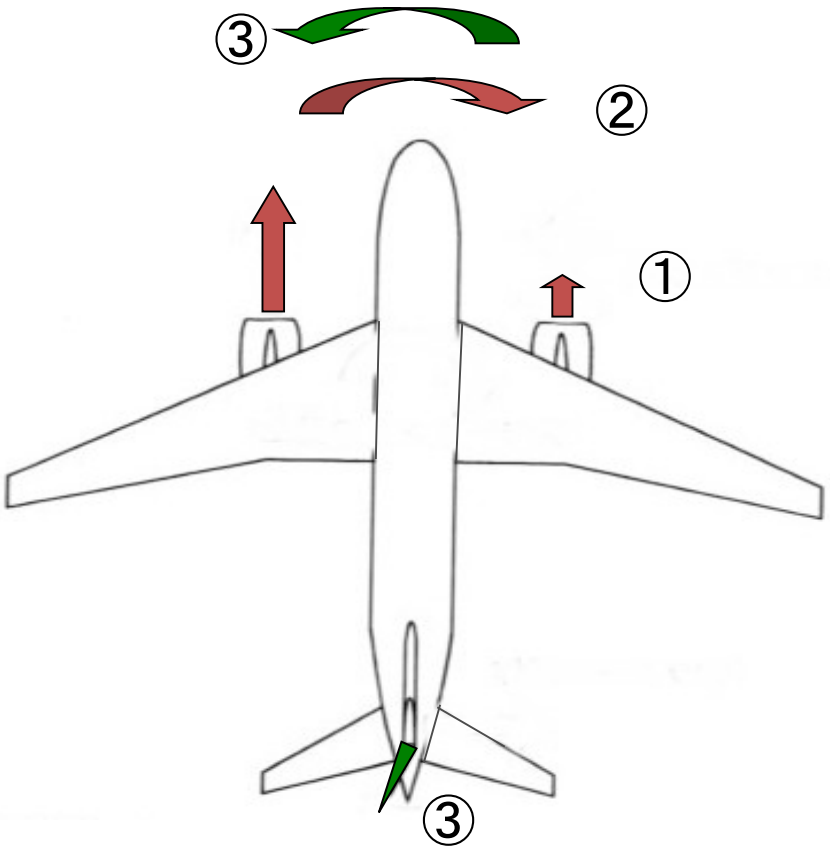
クルマが車線を逸脱しそうになると、警報と表示でドライバーに知らせ、
それと同時にステアリングを修正するトルクを発生する



LoA 6.5　システムはひとつの案を人に提示すると同時に、その案を実行

自動化レベル7：エンジン推力不均衡の補償

LoA 7　システムがすべてを行い、何を実行したか人に報告



① 第2エンジン（右主翼側）故障

② 左右エンジンの推力不均衡により機首が右に振れようとする

③ TACが方向舵を制御して機首を左に向ける力を作り出して②の力を打消し，機首の振れを抑制

Thrust Asymmetry compensation (TAC)

機械がよいと思ったことは、即時実行。人へは事後報告

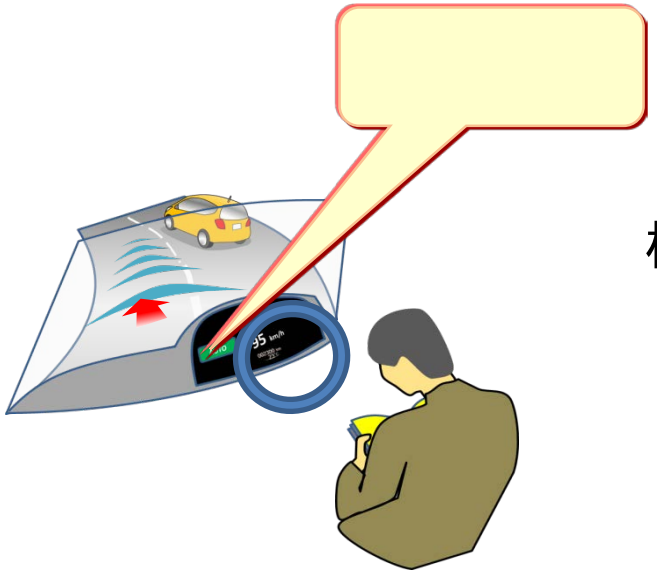
機械から人へ権限委譲を行いたいときの RTI は？

ユーザー：運転操作は行わず、走行環境の監視もしていない。
システムから運転交代を求められたとき、
瞬時に状況を見極め、適切に車両を制御する。

10秒後に運転を交代してほしいとき、
どのような要請にする？

120 km/h なら 333 m

60 km/h なら 167 m



システムから人へ
権限を円滑・安全に
移行させたい

機械から人へ権限委譲を行いたいときの RTI は？

基本形（SAE J3016）：　10秒以内に運転を交代してください

他のメッセージの可能性は？

自動化レベル（LoA）を参考に考案すると・・・

以下のような代替案が・・・

LoA 5 RTI　運転を交代してください。運転が引継がれたことが確認でき次第、自動走行モードを解除します

LoA 6 RTI　10秒以内に運転を交代してください。交代できない／交代したくない場合は拒否権を発動してください

LoA 6.5 RTI　直ちに運転を交代してください。今、まさに自動走行モードを解除しようとしているところです

Expected utility for an RTI

$$U(\text{Baseline}) = a\,P(\text{RD}|\text{Baseline}) - c\,P(\text{NR}|\text{Baseline})$$

$$U(\text{LoA 5}) = a\,P(\text{RD}|\text{LoA 5}) + b\,P(\text{NR}|\text{LoA 5})$$

$$U(\text{LoA 6}) = a\,P(\text{RD}|\text{LoA 6}) + b\,P(\text{VT}|\text{LoA 6}) - c\,P(\text{NR}|\text{LoA 6})$$

$$U(\text{LoA 6.5}) = \underline{a}\,P(\text{RD}|\text{LoA 6.5}) - c\,P(\text{NR}|\text{LoA 6.5})$$

where

RD: driver resumes driving NR: no response was given to the RTI

VT: driver vetoes the RTI

a : benefit of successful fallback by the driver

b : benefit of successful fallback by the automation

c : cost arising out of the state in which the vehicle is controlled neither by the automation or the driver

(Inagaki & Sheridan2017)

Order relations among design alternatives for RTI

U(LoA 6.5) < U(Baseline) < U(LoA 6) < U(LoA 5)

- LoDA 3 + Baseline RTI is not sensible.
- U(LoA 6) – U(Baseline) represents the *value of veto power*.
- LoDA 3 + LoA 5 RTI is optimal, but is outside LoDA 3.
- LoDA 3 + LoA 5 RTI is not equivalent to LoDA 4, meaning SAE's list of LoDAs in (SAE, 2016) is incomplete.
- LoDA 3 + LoA 5 RTI = High Automation in (SAE, 2014)
- Why not redefine LoDA 3 so that it can behave as High Automation in (SAE, 2014), or put the High Automation between LoDA 3 and LoDA 4 in (SAE, 2016)?

(Inagaki & Sheridan2017)

効用最大(リスク最小)の RTI

運転を交代してください。運転が引継がれたことが
確認でき次第、自動走行モードを解除します （LoA 5 RTI）

10秒経過後も、ユーザーが運転していることを確認できない

システムは「権限委譲は不可能」と判断し、
自身の機能範囲内で車両停止へ向けて制御を実行

上記形態は、「レベル3の自動運転」の範疇外

➡ レベル3の自動運転は、実現すべき目標として妥当か？

(Inagaki & Sheridan2017)

LoDA 4 – High Driving Automation (2016)

システム：　すべての動的運転タスクを担当。システム／車両の故障や想定作動環境からの逸脱等が発生しても、ユーザーの手助けを求めることなく適切に対応。

Photo: Volvo

- 「システムだけで対応できる」とは、「ユーザーに関与させない」こと？
- 何が起こっているか、システムがどのように対応しようとしているか等はユーザーに知らせる？　知らせない？

LoDA 4 – High Automation (2014) ← LoDA 3 + LoA 5 RTI

システムがすべての動的運転タスクを担当。システムが運転交代を要請してもユーザーが対応しないとき、システムは車両制御を継続。

自動運転システムの利用には、それなりの心構えが必要

Photo: BMW

Photo: Volvo

- 監視制御は、楽な仕事ではない
- 高機能なシステムの動作原理や能力限界を知らないと、システムを正しく監視することはできない
- 権限の的確な引継ぎには、瞬時の状況判断力が不可欠
- 自動運転の活用には、ドライバーも社会も意識改革が必要

誰のための自動運転？

- 自動運転がドライバーに何をもたらすか
  - 自動運転のレベルに依存
  - 誰を対象とするかに応じて適切な自動運転のレベル選定
  - 自動運転レベルが高いものが「レベルが高い」のではない
- 自動運転がドライバーに求めるもの
  - 自動運転のレベルに依存
  - ドライバーの役割を社会・ドライバーが認識する必要