中小企業における機能安全対応への取り組み

株式会社　サニー技研
尾仲 洋和、今村 聡彦

名古屋市工業研究所
小川 清、斉藤 直希

アジェンダ

1. 会社紹介
2. 中小企業を取り巻く機能安全対応の現状
3. サニー技研の機能安全対応活動紹介
4. 結果として得られたこと
5. まとめ

1. 会社紹介

会社概要

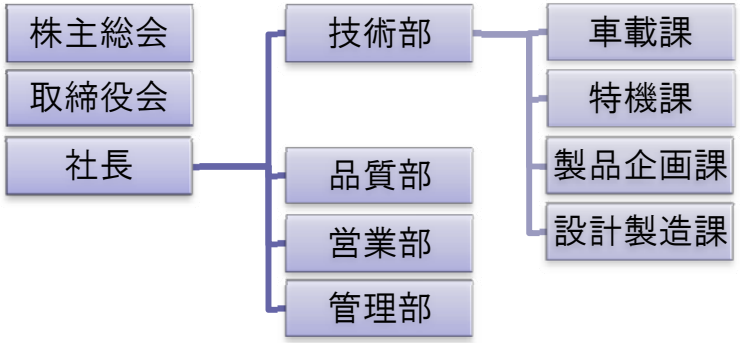
基本情報

・社名　　株式会社サニー技研
・所在地　　本社　兵庫県伊丹市
・代表者　　代表取締役社長　中村和彦
・設立　　１９７４年７月

事業内容

・【電子機器の開発、製造、販売】
　・マイクロコンピュータを応用した各種機器の開発・製造・販売
　・車載LANに関するツール開発・販売・適合試験
　・各種工場のFAシステム開発
　・情報通信機器のソフトウエアの開発
　・半導体試験装置の開発

組織図



加盟団体

・TOPPERS（正会員）
・ASIF（幹事会員）
　車載組込みシステムフォーラム
・JASPAR（正会員）
・AUTOSER
　（アソシエートメンバー）

事業所

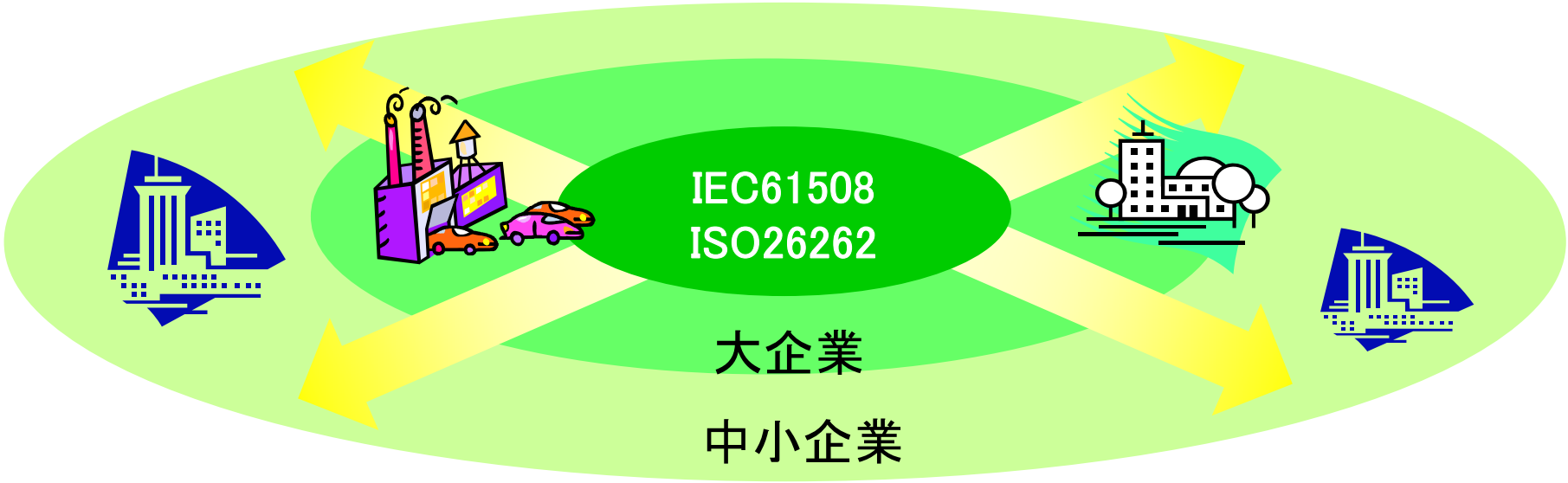
・本社/伊丹開発センター　　兵庫県伊丹市
・名古屋事業所/技術センター　名古屋市中区
・熊本技術センター　　熊本県熊本市

Sunny Giken Inc.

2. 中小企業を取り巻く機能安全対応の現状

中小企業を取り巻く機能安全対応の現状(１)

IEC 61508, ISO 26262などの電子機器とソフトウェアに対する機能安全規格の普及により、自動車などの安全関連製品に関わる中小企業も国際規格に適合した開発を実施する必要が出てきた。

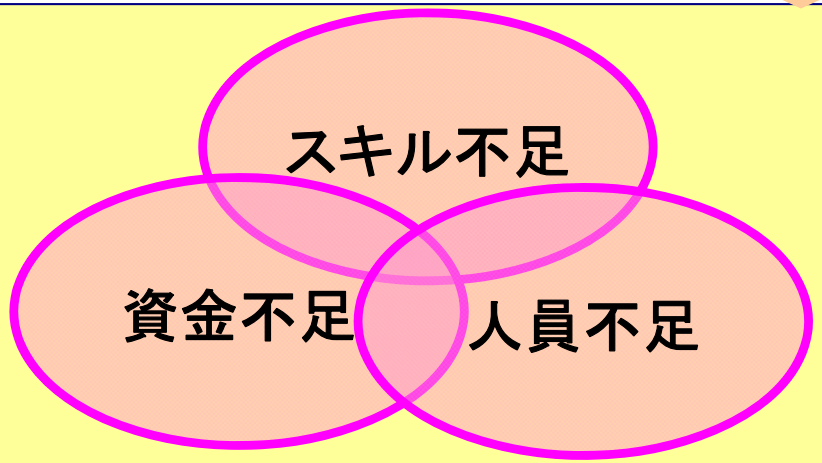


中小企業を取り巻く機能安全対応の現状(２)

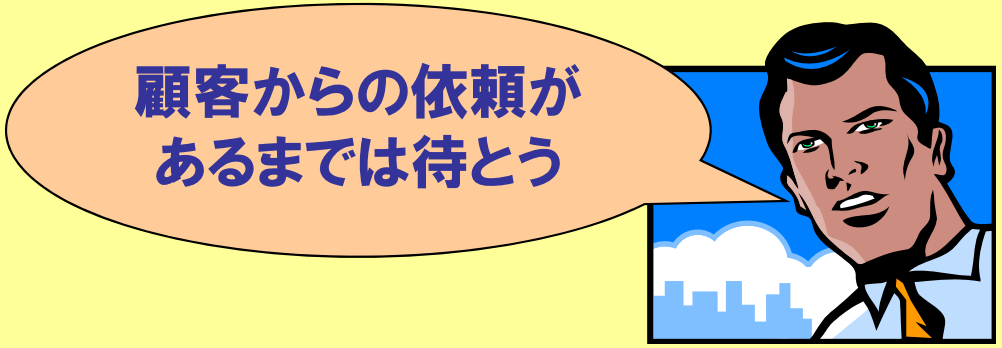
《機能安全に対する一般的な課題》

・機能安全規格に対応する中で、何から手を付けたら良いのかわからない。
・情報はあるが、人員・コストに負担が大きく、従来業務と並行して取組むにはリスクがある。
・コンサルタントに指導を受けるにしても、現状の自分たちのレベルがわからず、心配である。

それに加え中小企業で、抱えている課題

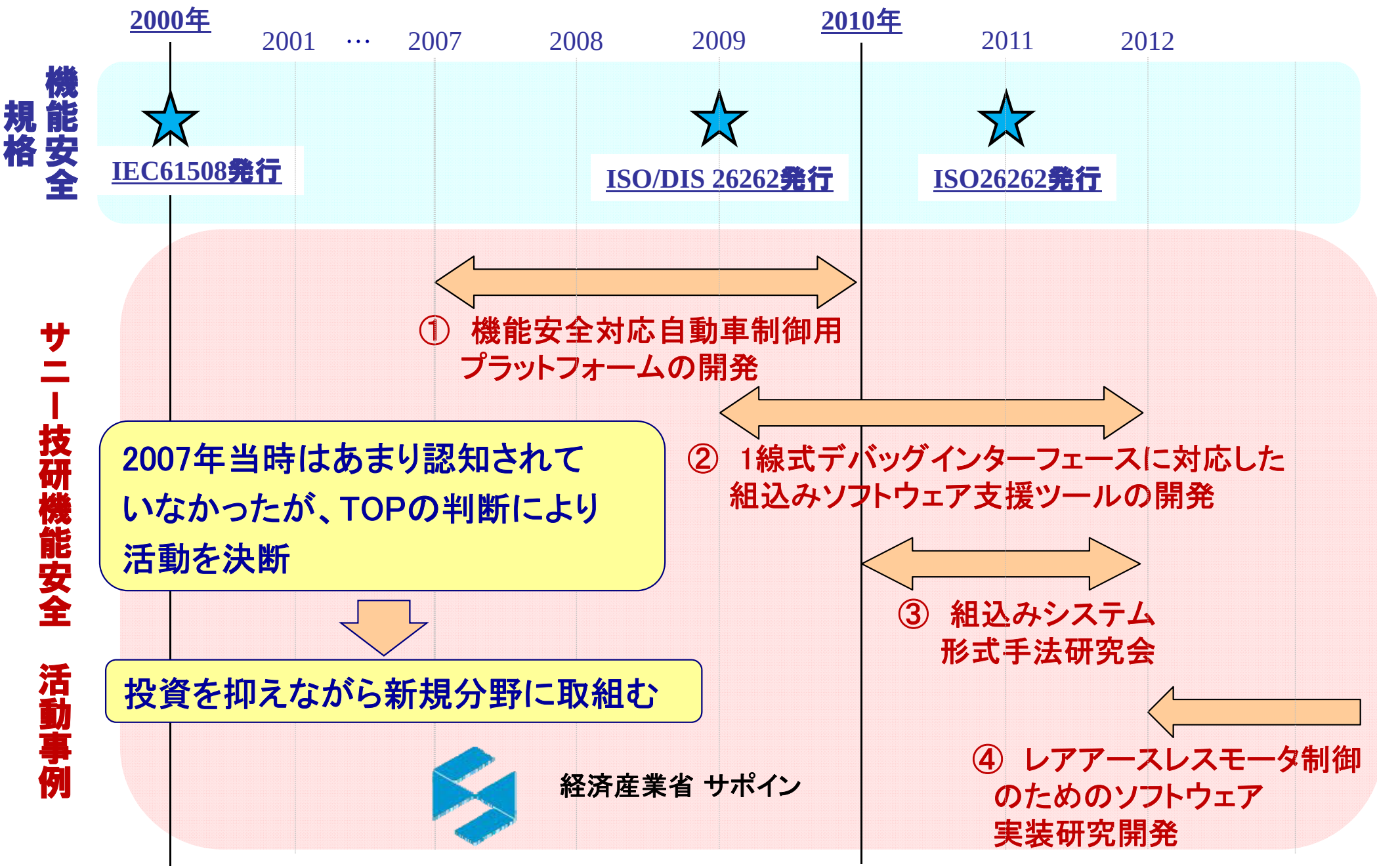


左記の3つの不足により



3. サニー技研の機能安全対応活動紹介

サニー技研の機能安全対応活動

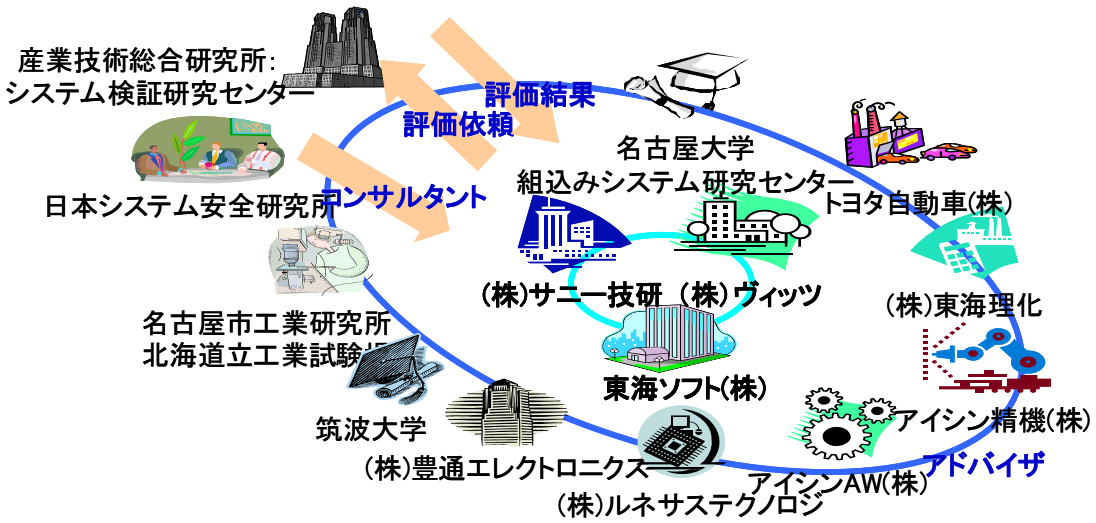


サポイン事業

■ サポイン事業による研究開発

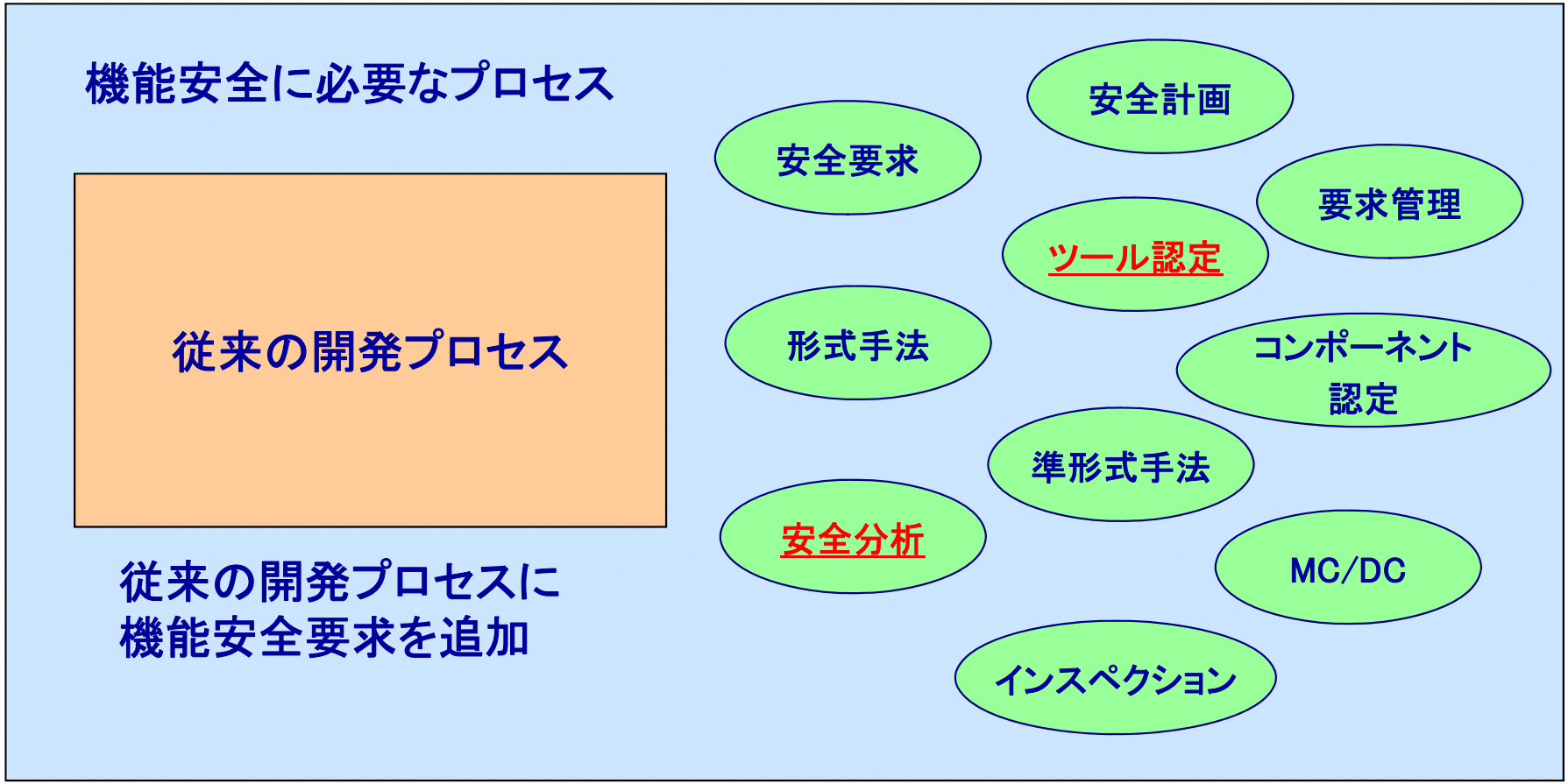
中小企業向けの公的資金援助を受け、産官学共同で研究開発を実施し、その中で、ソフトウェア/ハードウェア開発を通じて機能安全への理解と取り組むべきポイントの絞込みを達成。

※サポイン事業とは
経済産業省が実施している、戦略的基盤技術高度化支援事業の通称です。ものづくり基盤技術の高度化に向けて、中小企業が川下企業や研究機関等と協力して行う研究開発を支援するものです。



Sunny Giken Inc.

本活動における取組み

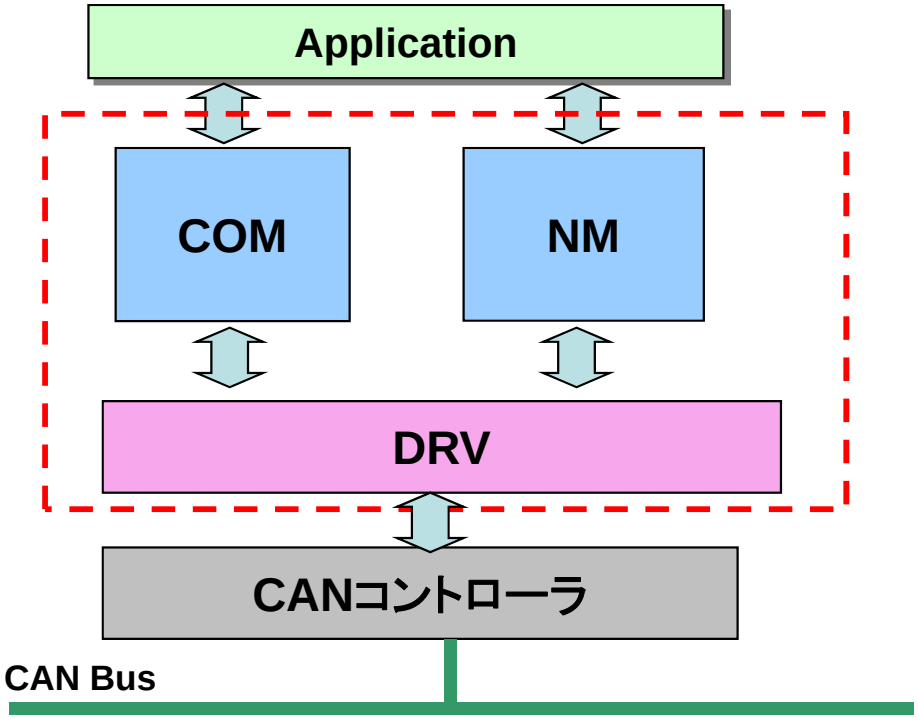


- 弊社では馴染みのない、新しい技術もあり、本活動を通じて実施してきた。
（安全分析：FMEA、FTA、HAZOP等）

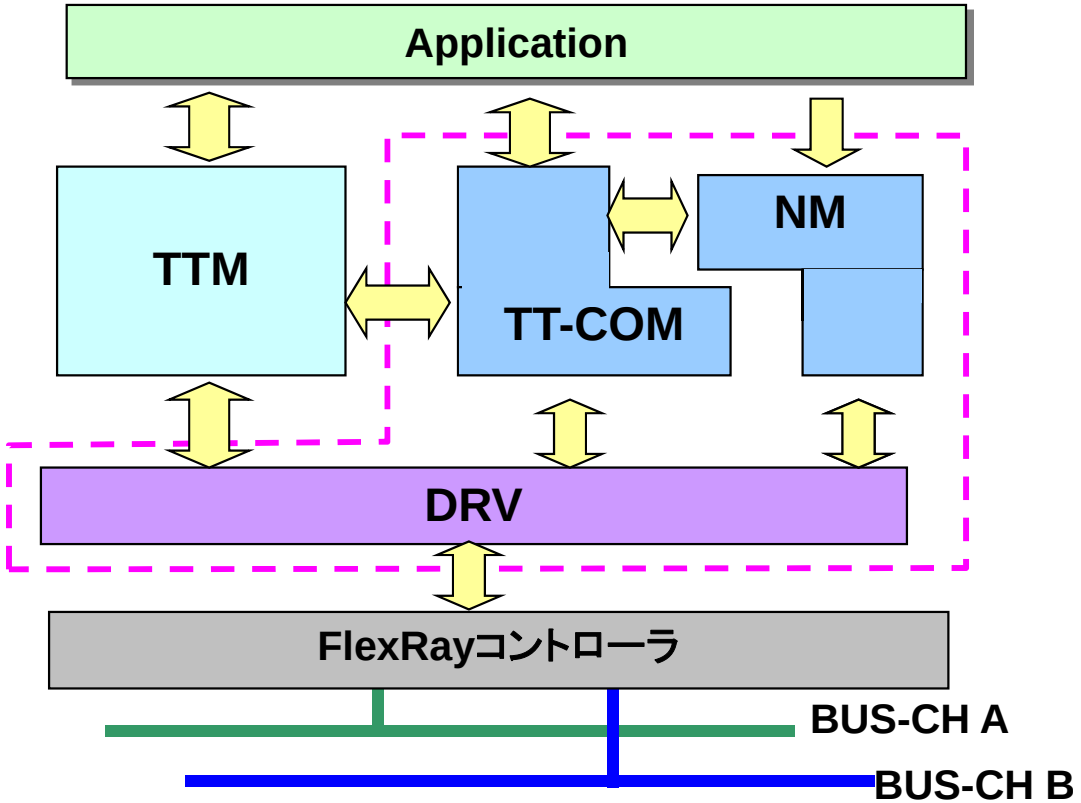
事例①

本活動における実施内容(安全分析)

「機能安全対応自動車制御用プラットフォームの開発」において、
CAN/FlexRay通信ミドルウェアの安全分析を実施



CAN通信ミドルウェア



FlexRay通信ミドルウェア

安全分析手順

以下の手順で、通信における安全分析を実施

①通信に使用されるシステムを以下の種類に分類する。
- ・通信路
- ・ハードウェア
- ・ミドルウェア
- ・アプリケーション

②それぞれの故障モードを以下の種類に分類し、原因,影響,対策の分析を行った。
- ・ノード（送信側）
- ・ノード（受信側）
- ・通信路

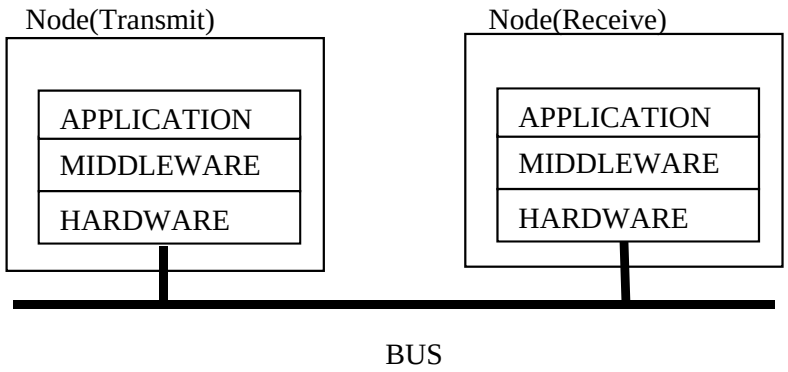
③脅威を受けた影響についての分析は通信ミドルウェア部分（①分類）を分析対象とし、
他の箇所は分析対象外とした。

④安全機能の防衛策を、以下のように分類する。

防止：　エラーの発生自体を防ぐ、もしくは緩和することができる防衛策。

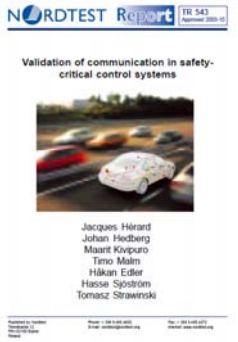
検知：　故障モードに対してエラーが発生したことを検出することができる防衛策。

軽減：　エラーの発生を防ぐことは出来ないが、
発生後にエラーに対してアプリへ
の影響を抑えることができる防衛策。



安全分析

故障モードは、「IEC 61784-3」や「Nord TEST ReportのValidation of communication in safety critical control systems」を参照した。



No.	Failuer mode 故障モード	Failure cause 故障原因		Failure effect 故障による影響	Protective method 防衛策
1	Repetition 重複	Transmit	アプリケーションからの過度な送信要求	バス負荷増加	[防止方法] 定期送信 [防止方法] イベントディレイ [検知方法] シーケンス番号
		Receive	–	–	–
		Bus	–	–	–
2	Deletion 欠損	Transmit	レジスタ故障	メッセージが送信されない	[防止方法] レジスタライトリードチェック [防止方法] レジスタリードチェック
			アプリケーションからの送信要求がこない	メッセージが送信されない	[防止方法] 定期送信
		Receive	受信メッセージの上書き	受信メッセージの取りこぼし	[検知方法] シーケンス番号
			レジスタ故障	受信メッセージの取りこぼし	[防止方法] レジスタリードチェック
		Bus	断線	受信メッセージの取りこぼし	[検知方法] 受信タイムアウト
			ノイズ	受信メッセージの取りこぼし	[検知方法] 受信タイムアウト
			ショート	受信メッセージの取りこぼし	[検知方法] 受信タイムアウト

安全分析で上がった防衛策の実装振り分け

具体的な防衛策の実装部

●：安全機能を実施する箇所
○：安全機能実施可能な箇所（ただし、他のモジュールで対応可能な機能のため未実施）

具体的な	Controller	MW			APL	Controller	MW			APL
		DRV	COM	NM			DRV	TT-COM	NM	
レジスタライト/リードチェック		●					●			
レジスタリードチェック		●					●			
定期送信機能			●		○	●				
送信間隔確保機能		○	●		○	●				
暗号化機能		○	○		●		○	○		●
ネットワークマネジメント				●	○				●	○
シーケンス番号			○		●			○		●
メッセージフィードバックチェック	●					●				
CRC	●	○	○		○	●	○	○		○
受信タイムアウトチェック			●		○			●		○
送信タイムアウトチェック			●		○			●		○
DLCチェック	●	○	●		○	●	○	●		○
データの多重化					●					●

本活動における実施内容(スキル定義)

※公的機関より指導を受けた内容(教育)

研究テーマ	公的機関	実施内容
機能安全対応自動車制御用プラットフォームの開発	名古屋市工業研究所	事業実施メンバーの教育およびスキル認定を実施し、教育するための実験教育を実施し、必要となる教育コンテンツを開発

《スキル表》

	スキルカテゴリ				支援のもとに作業を遂行で	自立的に作業を遂行できる	作業を分析し改善・改良できる	新たな技術を開発できる
	カテゴリ第1階層	カテゴリ第2階層	カテゴリ第3階層	説明	レベル1	レベル2	レベル3	レベル4
技術要素	測定	CANバス測定	バスモニタ	CAN専用バスモニタなどの機器を用いてCANバス通信の測定が出来る。				
	デジタル電子回路	CPU	R32C	R32Cに関した知識を持っている。また扱うことが出来る。				
	言語	C		C言語に関した知識を持っている。また扱うことが出来る。				
		アセンブラ		アセンブラに関した知識を持っている。また扱うことが出来				
	通信	CAN		CANに関した知識を持っている。また扱うことが出来る。				
開発管理	ソフトウェア詳細設計 コード作成 単体テスト	コード化		規定されたSW機能及び設計要求事項を、適当なプログラム言語を正しく使用することを通して、容易に理解でき分析可能なソースコードに翻訳することが出来る。関連するコーディング規格に該当の注意を				
		単体試験		開発したソフトウェアに対して試験仕様の策定が出来る。また試験仕様に基づいた試験を行うことが出来る。				
		MISRA-C		MISRA-Cを意識した開発が出来る。				
人間関係	指導力	意思決定		組織内・外に対して能力開発、時間管理、動機付けなどが出来る。				
	伝達	効果的伝達		組織内・外に対して情報伝達(話す・聞く・書く)が出来る。				
	交渉	働きかけと交渉		組織内・外に対して働きかけ・交渉(質問・調査・主張)が出来				
	問題解決			着眼、発想、問題解決、分析、論理思考などが出来る。				

事例②

本活動における実施内容(ツール認定)

「1線式デバッグインターフェースに対応した組込みソフトウェア支援ツールの開発」において、弊社製品RAMモニタのツール認定(ISO 26262 Part8-11)について調査を実施

《ISO 26262 Part8-11におけるツール認定》

- 機能安全開発内で使用する全てのツールは、使用する前にツールの信頼性を検証し、ツールの信頼性を確保してから使用することを求められている。
- ツールの信頼性を証明するには、ツールを使用するプロセスや、どういった機能を用いて、何をすることが目的であるのかということを明確しなければならない。そして、ツールを使用することによって安全にどのような影響を与えるのか、ツールの不具合を想定し、分析を行う。
- 分析した結果より、ツールに求められる信頼性レベル(TCL)を決定し、対応する信頼性の証明を行うことによって、ツールの使用可否を決定する。

TCLの求め方

TI(Tool Impact)	内容
TI1	ツールの不具合が、最終成果物に影響を与えない
TI2	ツールの不具合が、最終成果物に影響を与える

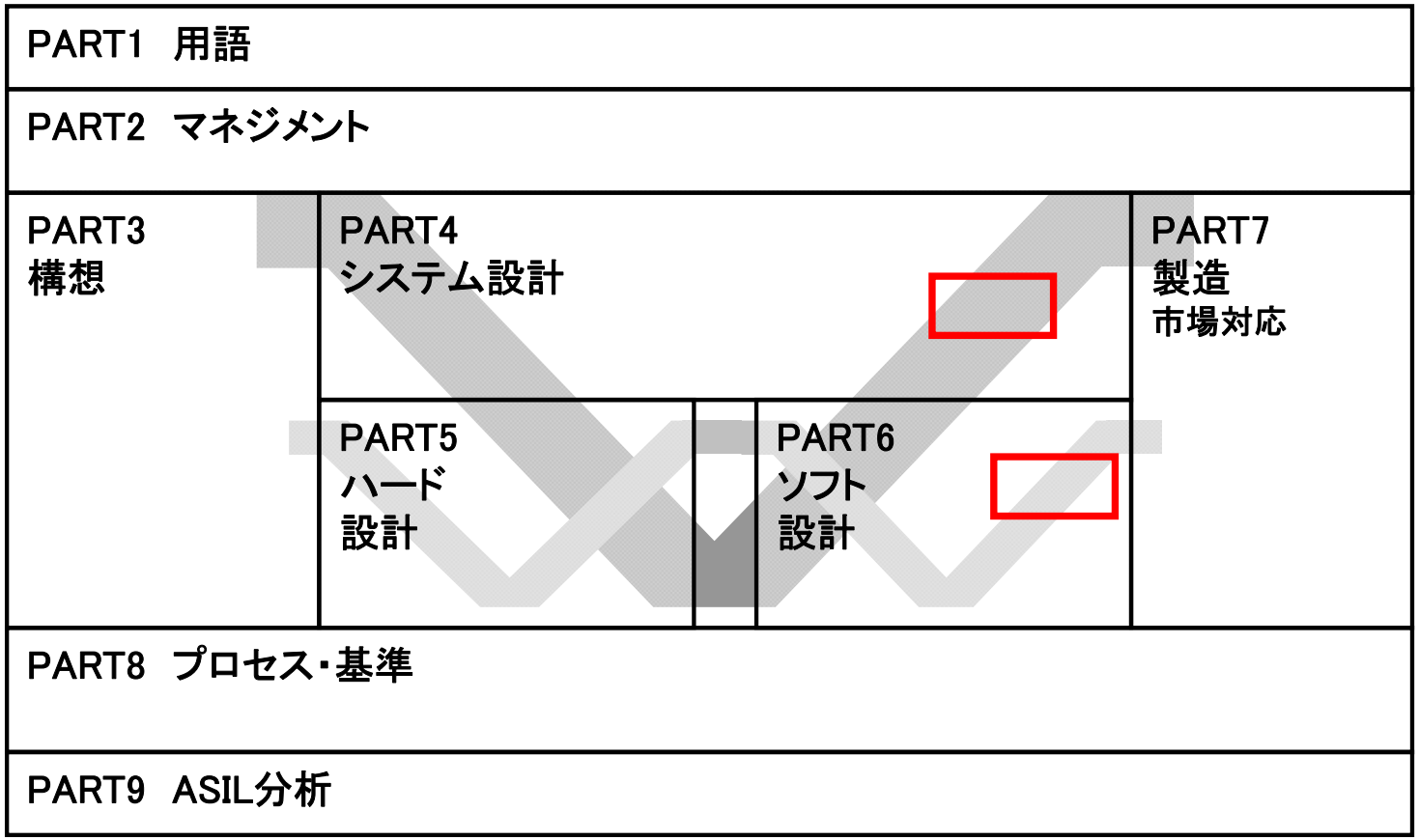
TD(Tool Error Detection)	内容
TD1	最終成果物に対して影響を与えるツールの不具合を検出する率が高い
TD2	最終成果物に対して影響を与えるツールの不具合を検出する率が低い
TD3	最終成果物に対して影響を与えるツールの不具合を検出しない

TIとTDの結果より、TCLが求まる。

	TD1	TD2	TD3
TI1	TCL1	TCL1	TCL1
TI2	TCL1	TCL2	TCL2

RAMモニタのユースケース

RAMモニタは、デバッグ・適合・検証で用いられるツールであり、赤枠で囲まれた箇所である、ソフトウェア結合テスト、システム結合テストにて用いられる。



RAMモニタの分析結果

分析結果より、RAMモニタは、プロセスにおいてBack to Backtテストを実施することを前提として、TCL1と判定

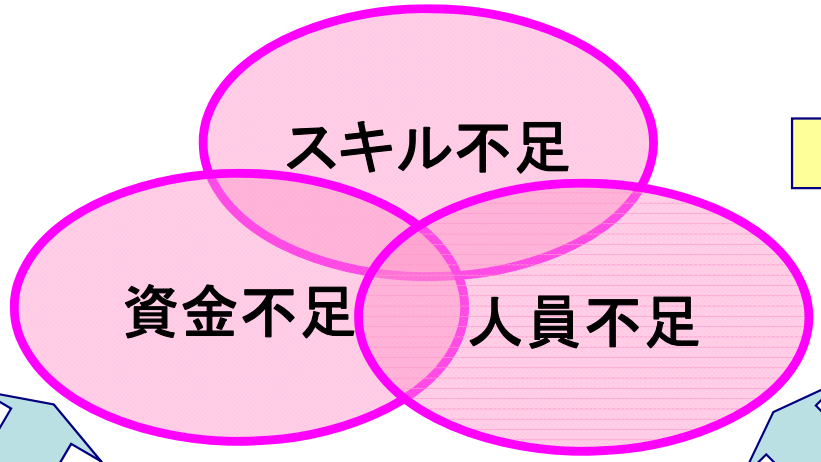
発表用資料にて表示します。

4. 結果として得られたこと

公的機関を活用することによるメリット

中小企業でも公的機関を活用して機能安全へ取り組むことが可能

自社以外の産官学の有識者が
参加されるため問題解消



中小企業でも、機能安全活動へ
の取組みは十分行える。

研究開発の資金援助が
受けられるため問題解決

人材を研究員として確保
することで問題解決

Sunny Giken Inc.

弊社の公的機関と連携した機能安全対応の環境

研究開発

経済産業省 サポイン
大学、公設研究機関、
アドバイザ企業他

JasPar
「ISO26262 実証実験WG活動」

知見

協力関係

プロセス認証取得支援
・㈱ヴィッツ
・産業総合研究所
・名古屋市工業研究所

協力関係

導入支援

プロセス認証取得支援
・分析、コンサル
・開発支援

サニー技研

発表

対外発表

TOPPERS
ASIF

社内取組み

公設研究機関、NPO法人による教育

マネジメント・品質・ハードウェア、ソフトウェアプロセスに関する規定を策定

・自社製品パイロット開発
・Automotive SPICE 研究活動

5. まとめ

まとめ

- 機能安全適合の開発を行うための準備が出来た。
  - 強みを活かした活動（通信の安全分析、マイコン開発環境）
  - 自社製ツールを機能安全対応へ向けて分析実施
  - ツールがどの工程で使用され、どれだけの安全対策が必要であるかの認識が出来、今後の開発にも繋がっている。
- 公的機関との活動の中で様々な分野の多くの方と出会うことが出来、技術的、システム的視野が広まった。
- 今後は本活動を通じて得たノウハウを活かし、公的機関と連携して顧客への提案やサービス提供を行い、さらに技術を高めたい。

参考文献

■中部組み込みソフトウェア技術者養成講座　プロダクトマネージャ育成、名古屋ソフトウェアセンター、2009

■プロセス改善ナビゲーションガイド　ベストプラクティス編、IPA/SEC、2008

■「中小企業の形式手法への取り組み 」発表資料、サニー技研、2011

■ Validation of communication in safetycritical control systems 、NORDTEST Report、2003

謝辞

本発表をするにあたり、機能安全活動ならびに名産研活動にご参加、ご指導を頂いたアドバイザ、大学、法人、企業の皆様に感謝申し上げます。

ご清聴ありがとうございました。