32SQiP 研究会　特別講義　レポート

作 成 日：　2016 年　6 月 13 日
書記氏名：　大島　修

日時	2016 年 6 月 10 日（金）　10:00 ～ 12:00
会場	(一財) 日本科学技術連盟・東高円寺ビル　2 階講堂
テーマ	「自動運転社会を見据えた組込み技術者のミッションとは? －君の開発したソフトウェアは、技術者として安全だ！と言える？言えない？－」
講師名・所属	小谷田　一詞　氏（一般財団法人日本自動車研究所 ITS 研究部 主席研究員）
司会者	三浦　邦彦　氏（矢崎総業株式会社）
アジェンダ	１．機能安全との出会い ２．信頼性と安全性 ３．自動車における機能安全とは ４．自動車用機能安全規格 ISO26262 ５．機能安全を通じて見えた物造りへのリスク ６．これからの自動運転社会に向けて
アブストラクト	「自動運転社会を見据えた組込み技術者のミッションとは?－君の開発したソフトウェアは、技術者として安全だ！と言える？言えない？－」と題して、自動車用機能安全規格 ISO26262 をベースに他業種との共通の考え方や手法を御教示頂きました。 特に「思いもよらないユースケースに対処する要件抽出と、要件に対する妥当性確認に命をかける活動が重要」と提言しており、システムアプローチのスキルを持ったシステム技術者を目指して欲しいと期待されております。 多種多様な分野の技術者、管理者が集まる中で「機能安全」の本質と他業種への展開の方向性について学んだ講演でした。ありがとうございました。

第 2 回の特別講演では、「自動運転社会を見据えた組込み技術者のミッションとは？－君の開発したソフトウェアは、技術者として安全だ！と言える？言えない？－」と題して小谷田さんから御講演を頂きました。
小谷田さんはパナソニック(旧松下通信)出身で ITS（Intelligent Transport Systems：高度道路交通システム）が特に強く、2012 年に「機能安全」をきっかけに JARI に転職されました。
システムの企画から運用までを担当し、気象庁、鉄道、空港、放送局、警視庁、カーナビ、ITS システム(AHS：自動運転の走り)等の実績があり、中でも車がとても好きで、自分で車検を取ってしまうほどであります。
今回は 2020 年に向けて自動運転が進んでいくので、「機能安全」という切り口で御講演頂きましたが、多種多様な分野の技術者、管理者が集まる中で自動車用機能安全規格 ISO26262 をベースに共通の考え方や手法を御教示頂きました。ありがとうございました。

１．機能安全との出会い
◆機能安全は何のため？
　→第三者への説明責任を果たすため。アセッサから指摘があってから資料を作るのはおかしくないか？指摘に対して、即設計書が出てくることを期待している。
◆ISO9000 は自分達が作ったものの品質を担保していることを確認するための道具、手段である。
　→「皆さんの活動の目的は何ですか？」手段と目的が逆転しないこと。ここを良く意識して欲しい。
◆ISO26262 is Japanese Supplier killer!!
　→ISO26262 は何のために開発されたか？を誰に聞いても明確に答えられない。
◆日本は規格に準拠させようとする。欧州は必ずしも規格に準拠する必要はなく、ベースとなる品質を担保した上で規格に準拠する。

２．信頼性と安全性
◆自分で実績を上げて来た結果（権利）がある為、若者に「何を考えて設計しているのか？」と言える。
◆昨日まで、ある会社でアセスメントをしてきたが、何でこんな設計になっているのか？という指摘に対して、エビデンスを示して欲しい。世のおじさん達はこれからの若い連中のために残して欲しい。
◆安全は、性悪説
　→こける、バグがある、故障する、ミスをする…
◆本質安全と言う言葉はリスクをゼロにすることを言う。用語としては、本質的安全が正しい。
◆現在は「安全」に関する学会がない。講師は早急に設立するよう提言している。
◆欧州のコンサルはテンプレートビジネス。この通りやれば良い。これで失敗したら、欧州のコンサルを選んだ方が悪い。
◆QMS はいかに開発現場が受け入れるか？がポイントである。現場が使えるものにすることを第一に考える。次回改善に向けて必ずアンケートを取ってフィードバックする。
◆2015 年度死亡事故が増加した。事故を如何にして減らすか？今、自動車業界は機能安全より、予防（能動的）安全に力を入れている。

３．自動車における機能安全とは
◆自動車業界では、OEM：自動車製造業者。トヨタ、日産、ダイムラー等の車両製造メーカー
　その下に Tire1：1 次下請け製造業者 DENSO、アイシン精機、BOSCH 等の部品製造メーカー
　その下に Tire2：2 次下請け製造業者 Tire1 にソフトウェアを供給するソフトウェアハウス
◆事故の危険性(リスク)を特定→分析→評価
　→自動車特有の安全分析・評価 ISO26262 Part-3 Concept Phase(フェーズ)
◆3.11 の原子力発電所の事故について、建てる時に機能安全の考え方はなかったのか？安全は 1 つ事故が起きると、これまでの安全が全てひっくり返る。
◆松下もパナソニックに変わったときに文化が変わった。だから、講師はあえて松下と言う。何かあったら隠蔽するのも会社の文化。
◆コントローラビリティ評価例
　→30 代の男性 25 名、50 代の女性 25 名をアルバイトで集めて、実際に評価してデータを集める。

◆ASIL は「安全機構（SM）や安全方策によって低減すべきリスクの大きさ」を表す。
◆H&R から安全目標導出までの流れ。安全目標→安全状態には停止、縮退、継続の 3 つがある。危険事象が発生してから安全状態へ持っていくのが、安全機構。
◆60km でコーナリング中にパワステが壊れた場合の例。日本は ASILD、欧州は QM。ドイツ人はコントローラビリティを重視。腕っ節が強いので、コントロールできると主張する。同じ事象でも組織によって考え方が違う。
◆カンファレンスは聞きに行くだけではだめ。話して情報を得ること。人と人は 50：50。決まったことを守るのが日本人。ドイツ人はどんどん先へ進める。
◆決定論的原因故障(システマティック故障)をいかに減らすかが重要。QM の世界で徹底的にたたく(排除する)。
◆ISO9000、ISO15504、CMM、CMMI、SPICE が QM。開発プロセスが大事。
◆ISO26262 を実施する第 1 ステップは SPICE 活動であると明言。
◆決して ISO26262 は Japanese Supplier Killer ではない。
　→安全であることの説明責任を果たすツール。安全に対する議論の文化が存在している、構築されている。
◆キーワードは State of the Art。これは覚えておく。

４．自動車用機能安全規格 ISO26262
◆ISO26262 規格の構造
　→Part1：用語集があるが、言葉の定義はとても重要である。言葉が合っていないと話が噛み合わない。
◆FIT 値：自動車は 1 ロット当たり何百万台でその内故障は 1～2 台程度である。
◆安全分析の手法として、HAZOP、FTA、FMEA がある。

５．機能安全を通じて見えた物造りへのリスク
◆日本の物造りはどうなんだ？
　→組込技術者とは「自動車に搭載される情報制御システムを開発している人」の意味。
　→要求に設計が混在している。要求は What、設計は How と言われる。
◆ドキュメントは重要。なければ、リバースで作る。設計書があるからテストができる、設計と違うからバグだと言い切れる。
◆品質を担保する特効薬はソフトを作らないこと。
◆HELLA：SEooC 開発では開発コストの削減、市場投入までの時間の短縮、保守作業の削減、複雑さに対処、開発コストの増加予測、顧客のメリットがある→競争力向上に繋がる。

６．これからの自動運転社会に向けて
◆IPA/SEC の資料。出荷後の不具合原因はソフトウェアの不具合が 40～50%。資料が古いので、本年度中に改訂して提示するとのこと。
◆自動車業界はソフトウェアに無関心。これから取り組む分野は、ソフトウェア満載。これをリスクと考えない、(良く分からない)文化。利益が計上されているうちは…。サプライヤは大変なことになるというリスクを持っている。
◆予防安全技術のてんこ盛り→自動運転へ
◆要件抽出⇔妥当性確認に時間を掛ける(時間が掛かる)、それ以外はドンと来いにしておかなければいけない。
◆もし自動運転になったら、妥当性確認に 11,415 年時間が掛かる。これまでは 41 日間。
◆「自動運転社会を見据えた組込み技術者のミッションとは？－君の開発したソフトウェアは、技術者として安全だ！と言える？言えない？－」
　→昔は、カンと経験と根性。ISO9000 認証を受けていれば、CMM、 CMMI、Automotive SPICE レベル 3(疑念だらけの認証)、ISO26262 準拠。

質問：講師が考えるアーキテクチャの意味とは？
→要求をどうやった手段で実現するか？作ったアーキテクチャに対して、特にパフォーマンスを気にする。理路整然と説明できること。組織も同様。アセスメントでは組織のアーキテクチャも見る。組織のアーキテクチャとソフトのアーキテクチャは一緒。美しいものから美しいものが出来上がる。