IPA Software Engineering Center
Information-technology Promotion Agency, Japan

形式手法適用調査

調査報告書

2010年7月29日

独立行政法人　情報処理推進機構
ソフトウェア・エンジニアリング・センター

目次

SEC
Software Engineering
for Mo・No・Zu・Ku・Ri

Software Engineering Center
Information-technology Promotion Agency, Japan

実応用プロジェクトリスト

実応用プロジェクトリスト

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

開発開始時期（製品発表時期等から推定）	開発対象（ドメイン）	開発組織	適用効果等	適用範囲／規模	期間	適用形式、ツールチェーン	プロジェクトチーム、スキル
2009/3-2010/2	プラットホームドア Sao Paulo METRO Line 2, 3, 4(鉄道)	ENGENHARIA E TECNOLOGIA LTDA TRENDS co. to POSCON(Korea)	RAMS SIL-3取得 短納期（3ヶ月）を実現	仕様、設計、実装、検証 10,000 LOC(C code)自動生成	3ヶ月（Poscon社での開発期間	SCADE	8(SW技術者 3, HW 技術者5)、形式手法経験なし
2009-2010	プラットフォームドア制御 Sao Paulo, Metro lines 2、3（鉄道）	TRENDS AeS ClearSy	SIL3取得 安全レベルの保証 コスト：2Mユーロ	仕様、設計、実装、検証	最初の1駅：1ヶ月	Atelier B	6名
2009-2010	SAET Paris Metro L1（鉄道）	RATP、STS				Atelier B	
2009	ホットフードベンディングマシーン（産業）	Sioux (Supplies software development services)	開発時間とコスト約30%削減 コスト：36,320ユーロ（学習時間含む）	モデリング、実装、検証 2889行（C#）	456時間（学習時間含む）	ASD（CSP） Verum ASD suite	
2009	列車搭載機器 Paris (Ouragan L3)（鉄道）	RATP、STS				Atelier B	

実応用プロジェクトリスト(続き)

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

開発開始時期(製品発表時期等から推定)	開発対象(ドメイン)	開発組織	適用効果等	適用範囲／規模	期間	適用形式、ツールチェーン	プロジェクトチーム、スキル
2009	軌道装置 Paris (Ouragan L3) (鉄道)	RATP、ANSALD				SCADE – Proof Toolkit	
–2009	CBTC Sao Paulo, METRO Line 4 (鉄道)	METRO SP、STS	SIL4取得			Atelier B	
2008	半導体ウェーハ測定器 (産業)	NandaTech	生産性向上 (約80 elocs／時) コスト:29,000ユーロ	モデリング 実装 検証 25,000 elocs(C++)	8週間	ASD(CSP) Verum ASD suite	平均1FTE
2008	デジタル病理評価機器 (医療機器)	Philips、ccm	FDA, ISO-13485取得 仕様品質、実装品質の向上	推定 60 – 90 KLoc	14ヶ月(プロトタイプ) 2ヶ月(HWインテグレーションとシステムテスト)	ASD(CSP) Verum ASD suite	約8500～13000 manhours
2008	列車保全安全制御システム:Train Protection System – Seoul (鉄道)	Alstom、ClearSy		62 kloc B 33k loc ADA		Atelier B	

実応用プロジェクトリスト(続き)

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

開発開始時期(製品発表時期等から推定)	開発対象(ドメイン)	開発組織	適用効果等	適用範囲／規模	期間	適用形式、ツールチェーン	プロジェクトチーム、スキル
2008	列車保全安全制御システム:Train Protection System - Delhi (鉄道)	Alstom、ClearSy		62 kloc B 33k loc ADA		Atelier B	
2008	列車保全安全制御システム:Train Protection System - Santiago (鉄道)	Alstom、ClearSy		62 kloc B 33k loc ADA		Atelier B	
2008/9-	X線CTスキャン(医療機器)	Philips Healthcare Cardiovascular division	2ヶ月のデータ収集期間(69人日)に、387の不具合発見 コスト:541,161ユーロ	27381 LOC (7,697 C++, 19,684 C#)	2ヶ月	ASD(CSP) Verum ASD suite	チーム1:1.5 SW技術者 (C++) チーム2::5 SW技術者 (C#) 形式手法経験なし
-2008	CBTC Sao Paulo METRO Line 2 (鉄道)	METRO SP、Alston	SIL4取得			Atelier B	
2008	A400M Low Alt. FC, Fuel Managment, HLC, CDS, & Navigation(航空宇宙)	EADS、Sagam、Intertechnique、Saab、Thales				SCADE	

実応用プロジェクトリスト(続き)

SEC
Software Engineering
for Mo・No・Zu・Ku・Ri

開発開始時期(製品発表時期等から推定)	開発対象(ドメイン)	開発組織	適用効果等	適用範囲／規模	期間	適用形式、ツールチェーン	プロジェクトチーム、スキル
2008	Sikorski S76 Flight controls, FADEC & CDS(航空宇宙)	Avionika P&W Canada Thales/Diehl				SCADE	
2007-	オランダ運河のマエスラント防潮可動橋(水門)(Maeslantkering)の意志決定システム(BOS)	国家水路・水事業保全省 Logica	アップグレード(新規ハードウェアへのポーティング)			Z Promela／SPIN	
2007	FDIR strategy (Failure Detection, Isolation and Recovery)(航空宇宙)	CNES Thales Alenia Space ClearSy		検証		B	
2007	Redevelopment CDIS(CCF Display Information System)(航空宇宙)	(EU RODIN project)	15年前にPraxisにより開発されたCDISの再構築	抽象モデル:4ページ		Event B Rodin tool	
2007	Boeing B787 Braking System	Boeing Messier Bugatti (France)				SCADE	

実応用プロジェクトリスト(続き)

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

開発開始時期(製品発表時期等から推定)	開発対象(ドメイン)	開発組織	適用効果等	適用範囲／規模	期間	適用形式、ツールチェーン	プロジェクトチーム、スキル
2007	Boeing B787 着陸ギアシステム(航空・宇宙)	Boeing Smiths Aerospace(英)				SCADE	
2007	フラッシュメモリデバイスドライバ(半導体)	三星電子	フラッシュメモリを制御するドライバ、小規模だが複数レイヤの複雑な構造をしており検証が必要	検証 200LOC		NuSMV SPIN CBMC	
2007	PW535E & PW617F FADEC(航空宇宙)	P&W Canada				SCADE	
2007	列車保全安全制御システム:Train Protection System – Milan (鉄道)	Alstom ClearSy		112 kloc B onboard, 118 kloc B trackside		Atelier B	
2007	列車保全安全制御システム:Train Protection System – Malaga (鉄道)	Alstom ClearSy		112 kloc B onboard, 118 kloc B trackside		Atelier B	

実応用プロジェクトリスト(続き)

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

開発開始時期(製品発表時期等から推定)	開発対象(ドメイン)	開発組織	適用効果等	適用範囲／規模	期間	適用形式、ツールチェーン	プロジェクトチーム、スキル
2001～2006(就業2006)	CBTC New York Line L(鉄道)	New York City Transit (NYCT) Siemens Transportation Systems		仕様、実装、検証 110,000 行自動コード生成 82,500 証明責務		Atelier B AdaCore EDiThB(STS)	
2006	シャルルドゴール空港の無人シャトル制御(Roissy WCU-SCS project)(鉄道)	ADP(Paris Airport) Siemens Transportation Systems ClearSy	開発されたソフトウェアはIEC61508: EN50126、EN50128,、EN50129に準拠し、SIL4に分類された。	機能仕様、実装、検証 28,000+155,000行(B) 43,000 証明責務 158,000行(Ada)		EDiTh B Bertille Atelier B/ClearSy	
2006	既存の地下鉄駅へのプラットホームドア設置(鉄道)	RATP ClearSy KABA	48 000回の開閉命令で不具合0	システム機能仕様:130P、セーフティケース:300P 開発書類:600頁、証明責務:500、モデル:4000行	合計:9ヶ月 event-Bモデル:3ヶ月 信頼性事前検証:8ヶ月	COMPOSYS B4Free(FreeSoftware) Atelier B	ClearSy(4名)、PM:SW開発経験5年、安全技術者:シニアレベル、開発技術者:ジュニアレベル、検証技術者:ジュニアレベル
2006	ブレーキシステム(鉄道)	Siemens Transportation Systems	ブレーキシステムの障害可能性分析	設計		FTA(Fault TreeAnalysis) Fault Tree generation tool	
2006	船舶通信システム(通信)	Selex Communications、University of L'Aquila(イタリア)	状態数を大幅に削減し、すべての性質を検証できた	アーキテクチャモデル検証		ADL、Promela、UML CHARMY、SPIN、DEPCOL、TESTOR	

実応用プロジェクトリスト(続き)

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

開発開始時期(製品発表時期等から推定)	開発対象(ドメイン)	開発組織	適用効果等	適用範囲／規模	期間	適用形式、ツールチェーン	プロジェクトチーム、スキル
2006-2010	Jet engine EMU(航空宇宙)					SPARK	
2008年	Train Protection System(北京地下鉄10号線)(鉄道)	ClearSy、ALSTOM	安全性、信頼性、すべての機能を再形式化	要求仕様、実装、検証		B method	
2006	M88-2 FADEC(航空宇宙)	Dassault Aviation				SCADE	
2006	PW6A67 & PW535B FADEC(航空宇宙)	P&W Canada				SCADE	
2006-2007	Trusted Services Engine (TSE) is a network (セキュリティ)	SPAWAR NSA Galois	EAL6	モデリング、検証		QuickCheck tool	

実応用プロジェクトリスト(続き)

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

開発開始時期(製品発表時期等から推定)	開発対象(ドメイン)	開発組織	適用効果等	適用範囲／規模	期間	適用形式、ツールチェーン	プロジェクトチーム、スキル
2007	列車保全安全制御システム:Train Protection System – Incheon (鉄道)	Alstom ClearSy		62kloc B、33kloc ADA		Atelier B	
2006	KFS (automatic stop at signal)(鉄道)	VOSLO (Vossloh) ClearSy				Atelier B	
2005-進行中	iFACT、航空管制システム(航空宇宙)	NASTIONL Air Traffic Services(NATS) Praxis Lockheed Martin	障害、不具合の削減 10百万ポンド:航空管制システム全体 5百万ポンド (Praxisとの契約額)	仕様、実装、検証 仕様:Z表記と英語 コーディング(150kloc:SPARK/Ada、25kloc:C)	2年間	AdaCore GNAT Pro compilers SPARK Fuzz for Z (Oxford Univ.)	20名:機能仕様 115:実装(ピーク時) テスト/検証:50/50 NATSとPraxisの技術者 20 (Zの読書き) 50 (Can read Z) 一般的比率 レベルA:20%、レベルB:30%、レベルC:50%
2005-2007	航空機ソフトウェアの汎用的な電子配布システム(AADS)(航空宇宙)	Boeing, Washington大学(米) Siemens(独)	電子配布されるソフトウェアのセキュリティを確保するシステムの開発	要求分析、検証	3年間	AVISPA(プロトコル検証ツール)	

実応用プロジェクトリスト(続き)

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

開発開始時期(製品発表時期等から推定)	開発対象(ドメイン)	開発組織	適用効果等	適用範囲／規模	期間	適用形式、ツールチェーン	プロジェクトチーム、スキル
2005-2006	PWC 535B Engine(航空宇宙)	Pratt & Whitney	コードレビューなし、統合テストなし、自動コード生成			SCADE	
2005	分散RTOS (OpenComRTOS) (その他)	Altrenic、Open Licence Societyのスピンオフ	「Correct(リードエラーなし、クリーン)」ネットワークOSの開発 小サイズ 効率的開発	仕様、設計、実装ー1KB以下(コンパイル後)ANSI-C (Misra確認) モデル20-30ページ	12ヶ月	TLA+/TLC	シニアアーキテクト(Phd) 電子、メカ技術者(FM経験なし)
2005	PW610 & PW615F FADEC(航空宇宙)	P&W Canada				SCADE	
2005	列車保全安全制御システム-Cairo (鉄道)	Alstom ClearSy		62 kloc B, 33k loc ADA		Atelier B	
2005	列車保全安全制御システム-Madrid(鉄道)	Alstom ClearSy		62 kloc B, 33k loc ADA		Atelier B	

実応用プロジェクトリスト(続き)

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

開発開始時期(製品発表時期等から推定)	開発対象(ドメイン)	開発組織	適用効果等	適用範囲／規模	期間	適用形式、ツールチェーン	プロジェクトチーム、スキル
2004	鉄道制御システム-Sanjuan (鉄道)	Puerto Rico Highways and Transportation Authority STS		79ファイル 23,000行(B)		AtelierB	
2004-2006	フェリカチップ	フェリカネットワークス	仕様の明確な定義 デバッグ密度 = 440/40,000 =約 11エラー/kLOC	形式仕様:約100,000 LOC、含むテストケース:約60,000 LOCとコメント C++:110,000 LOC	2年間	VDM Tool	50名
2004	Eurocopter EC225 Autopilot(航空宇宙)	Eurocopter				SCADE	
2004	鉄道制御システム-Caracas (鉄道)	STS				AtelierB	
2004	鉄道制御システム-Lausanne (鉄道)	Alstom ClearSy		108Kloc B		AtelierB	

実応用プロジェクトリスト(続き)

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

開発開始時期(製品発表時期等から推定)	開発対象(ドメイン)	開発組織	適用効果等	適用範囲／規模	期間	適用形式、ツールチェーン	プロジェクトチーム、スキル
2003-2004	プレス制御(産業)	INRS (French Institute for Workers Safe) ClearSy	プレス制御装置の安全設計	仕様、実装、検証		B	
2003	スマートカード(セキュリティ)	Gemplus	検証コスト削減 EAL5認証 バグ件数:95ー>74 開発期間:17週ー>20週	仕様、実装、検証	20週間	B	
2003	Tokeneer ID Station (TIS) プロジェクト(セキュリティ)	NSA Praxis HIS SPRE	品質保証レベル5(EAL5)の高品質、少欠陥のシステム開発	仕様、実装、検証 開発行数:9939行 開発日数:260日 生産性:38行／日 納入後不具合:0／1000行	9ヶ月/260人日	SPARK	3名 A レベル　2名 Bレベル　1名
2003	列車保全安全制御システム-大邱市 (鉄道)	Alstom ClearSy		62 kloc B, 33k loc ADA		Atelier B	
2002	列車保全安全制御システム:Train Protection System - Shangai (鉄道)	Alstom ClearSy		62 kloc B, 33k loc ADA		Atelier B	

実応用プロジェクトリスト(続き)

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

開発開始時期(製品発表時期等から推定)	開発対象(ドメイン)	開発組織	適用効果等	適用範囲／規模	期間	適用形式、ツールチェーン	プロジェクトチーム、スキル
2002	列車保全安全制御システム-Istanbul (鉄道)	Alstom ClearSy		112 kloc B onboard, 118 kloc B trackside			
2002	航空機テストセット	General Dynamics UK Praxis	28 LOC/Day <0.1 defects/ksLOC	35,000 LOC		SPARK Z	
2001-2007	ジェットエンジンEMU					SPARK	
2001-2005	Falcon F7X デジタルフライトコントロール ブレーキシステム	Dassault Aviation	ソースコードレビュー、統合テストなし 開発サイクル45%短縮	95%コード生成 (30 000 lines C) (DFC)		SCADE	
2001	MULTOS認証システム (Global Key Center)	Mondex International Praxis HIS	マルチアプリケーションOSの開発	要求仕様、実装、テスト		SPARK 30% Ada95 30% C++ 30% C 5% SQL 5%	

実応用プロジェクトリスト(続き)

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

開発開始時期(製品発表時期等から推定)	開発対象(ドメイン)	開発組織	適用効果等	適用範囲／規模	期間	適用形式、ツールチェーン	プロジェクトチーム、スキル
2001	Hongkong Railway systems(鉄道)	MTRC STS				B	
2001-	Aermacchi M346(航空宇宙)	AerMacchi.				SCADE	
2000～2001	Trade One証券(バックオフィス・システムのパッケージ)のサブシステム	CSK(日本フィッツ)	曖昧な仕様に起因するトラブルを防ぐ リリース後欠陥ゼロ 単体テスト以前の欠陥の原因 57	機能仕様の検証、詳細設計 1.3MLOC		VDMTools(IFID)	
2000	Eurocopter EC145 Autopilot(航空宇宙)	Eurocopter				SCADE	
2000	Mexico鉄道システム(鉄道)	STS				B	

実応用プロジェクトリスト(続き)

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

開発開始時期(製品発表時期等から推定)	開発対象(ドメイン)	開発組織	適用効果等	適用範囲／規模	期間	適用形式、ツールチェーン	プロジェクトチーム、スキル
2000	列車保全安全制御システム-Singapour(鉄道)	Alstom ClearSy		108K loc B, 105 kloc Modula2		Atelier B	
1990年代後半から2005年	航空機(A380)フライトガイダンスシステム他(航空宇宙)	Airbus	コード自動生成(70%自動生成)による開発サイクルの短縮 仕様変更への迅速な対応	仕様、実装、検証 785,000LOC (Flight Control Guidance Unit)		SCADE Prover Plug-In enables verification tool	
1999-2001	自動車サブシステム(ライト、エアバッグ、エンジン …)(産業)	Peugeot Automobiles ClearSy	サブシステムの機能モデル 仕様の一貫性、明確化を実現	機能モデル　約2 x 150,000行のドキュメント生成		Atelier B	
2000	Vital Settings Generator(鉄道)	ALSTOM ClearSy	統合テストなし	75 000行(B) 52 000行(Ada)	5ヶ月		低スキル(ジュニア):1名 平均スキル:1名 専門家:1名
1999	SPOT 4 (航空宇宙)	CS-CI(仏)	(SPOT4衛星のペイロード)	ソースコード行数38%削減 工数36%削減 自動コード生成:C++		IFAD VDM-SLツールボックス	

実応用プロジェクトリスト(続き)

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

開発開始時期(製品発表時期等から推定)	開発対象(ドメイン)	開発組織	適用効果等	適用範囲／規模	期間	適用形式、ツールチェーン	プロジェクトチーム、スキル
1998	フラワーオークション(金融)	Chess(蘭)	UMLとVDM++の利用			The IFAD VDM++ツールボックス	
1998-	CAVA(エンタプライズ)	Baan (デンマーク)	制約ソルバ(営業構成管理) 早期のテスト開始 複雑システムの品質改善と開発リスク低減			The IFAD VDM++ツールボックス	
1997-1999	民間ヘリコプタ機の自動パイロット(EC135、EC155)(航空宇宙)	Eurocopter SFIM	自動コード生成:90%、開発時間1/2 EASA認証(EC155, EC135, EC145, EC225)、TAT短縮	33,500行自動コード生成		SCADE	
1997-1998	オランダ DoDのシステム(防衛)	Origin(蘭)	期待してコストでのデリバリ デリバリ後コードエラー発見されず	仕様:151行 マニュアル実装:4KLOC 自動実装:90 KLOC 合計:94KLOC	仕様:1,196時間 マニュアル実装:471時間 テスト:612時間 合計:2,279時間	IFAD VDM-SLツールボックス	
1997	BPS 1000 紙幣処理(金融)	GAO(独)	センサデータの把握 保守時間の節約 エラーの発見			IFAD VDM-SLツールボックス	

実応用プロジェクトリスト(続き)

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

開発開始時期(製品発表時期等から推定)	開発対象(ドメイン)	開発組織	適用効果等	適用範囲／規模	期間	適用形式、ツールチェーン	プロジェクトチーム、スキル
1996-1997	SHOLIS(ヘリコプタ着陸システム)(防衛)	UK MOD PMES Ltd Praxis	離着陸の安全情報の確認 SIL4 Defect/ksLOC:0.22 LOC/Day:7	Z 仕様:200ページ Spark:27,000 LOC		Z SPARK CADiZ	
1995-1997	DustExpert Safety (dust explosives)(公共)	Adelard (英)	納期内に予定したコストで納入 テストプロセスの効率化	初期仕様 450ページ VDM仕様 16kloc C++ GUI:23kloc 実装:18kloc		The IFAD VDM-SL ツールボックス	プロジェクトマネージャ/開発技術者/設計専門家/ISA技術者 x 2
1995-1996	オランダ運河のマエスラント防潮可動橋(水門)(Maeslantkering)の意志決定システム(BOS)(公共)	国家水路・水事業保全省 CMG Den Hagg BV	IEC61508/SIL4	29プログラム:20,000行、Operational System:200KLOC、Simulator/Test System: 250KLOC		Promela (Promela/SPIN) Ward & Mellor(Case Tool, Z) LaTex(ドキュメント)	
1995年	Lockheed C130J ミッションコンピュータ(航空宇宙)	Lockheed Martin Praxis	DO-178Bに必要なテストコスト削減 V&Vコスト削減 UK MoD と FAAの認定要求合致	仕様、設計、実装、テスト 130,000LOC		Z SPARK	
1994-1998	鉄道制御システム(パリ地下鉄14号線)(鉄道)	RATP(仏) MATRA(仏)	RATPによる義務付け(B)、証明後、機能検証、統合検証、オンサイトテスト、運用でバグ発見されず	仕様、実装、検証 107,000行(B)、 29,000証明責務 87,000行(Ada)	4年(最初の形式手法プロジェクトであったため4年かかった)	Atelier B	RATP (仕様、妥当性検証):15名 STS (モデル化、妥当性検証、コード生成、テスト):35名

実応用プロジェクトリスト(続き)

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

開発開始時期(製品発表時期等から推定)	開発対象(ドメイン)	開発組織	適用効果等	適用範囲／規模	期間	適用形式、ツールチェーン	プロジェクトチーム、スキル
1994	ゲートウェイ(Conform Project)(セキュリティ)	British Aerospace (英) IFID(デンマーク)	安全系システムの生産性向上、障害密度改善			VDM-SL Toolbox (IFAD)	
1992-1996	航空管制システム(航空宇宙)	Praxis(英)	形式記述の再構築と新規ツールの適用 不具合数の大幅な削減(0.75/1000行)	仕様、設計 仕様:1200ページ 設計書類:約3000ページ		VDM VVSL(VDMの派生) Event B	
1990年前半～1999年	MULTOS OSとパースアプリケーション(セキュリティ)	National Westminster Bank Platform Seven Logica University of York	ITSEC level E6認証、納入1年後までの欠陥:4個	100,000行、フォーマルセキュリティポリシ(Z)、機能仕様:500頁(Z)、並行設計:CSP+モデルチェック	3500人日、27 loc／日	Z CSP	
1992年	CDIS(CCFディスプレイ情報システム)(航空宇宙)	Praxis UK Civil Aviation Authority	不具合数 0.75／1000行 FM未使用の場合より2倍から10倍少ない。12.7LOC/day(生産性)	実装、検証 197000LOC(行数)		VVSL (Variant of VDM)	
1991-1993	Flight Warning Computer (FWC) Airbus 330/340(航空宇宙)	Airbus	不具合数削減による開発費削減、初期仕様と詳細仕様への適用適用困難、従来方法の代替とはならない	プロトタイプ、検証		C sar/Ald ebaran toolset for Lotos	

実応用プロジェクトリスト(続き)

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

開発開始時期(製品発表時期等から推定)	開発対象(ドメイン)	開発組織	適用効果等	適用範囲／規模	期間	適用形式、ツールチェーン	プロジェクトチーム、スキル
1991-1992	CDTC(鉄道)	MRC GEC Alstom				B	
1990-1994	HDMS-A; 医療情報システム(医療)	Korso Project(ドイツの産学共同プロジェクト)	形式手法の手法、言語、ツールの開発 大規模医療システムへの形式手法適用事例研究成果	大規模医療システムの機能モデル仕様記述		Petri net(Others)	
1990-1993	キャビン通信システム(A330/A340)(航空宇宙)	DST Deutsche System(for Daimler-Benz、Airbus、KID-Systeme)	安全、高信頼性システムの開発、品質 ソフトウェア品質が大幅に改善された DOD178B	仕様、実装、検証 注釈付Z仕様:35頁 アプリ:6,000行(C) 機能数:95		Z	
1990	Eurofighter Typhoon(防衛)			5百万行		Z SPARK	
1990年代前半	鉄道管理システム(ERTMS/ETCS)(鉄道)	Rete Ferroviaria Italiana(イタリア)	RAMS(国際鉄道標準)へ対応するための機能的テスト仕様の解析	設計、テスト 要求の検証を行い、テストフェーズの計画と素早い問題の解決を実現		Statemate(ステートチャートによる仕様記述、分析ツール)	

実応用プロジェクトリスト(続き)

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

開発開始時期(製品発表時期等から推定)	開発対象(ドメイン)	開発組織	適用効果等	適用範囲／規模	期間	適用形式、ツールチェーン	プロジェクトチーム、スキル
1988-1990	医療機器分析情報ベース(AIB)コンピュータモニタリング(医療)	HP	FM記述仕様による技術トランスファ タイムツーマーケット未達、品質大差なし	要求仕様 設計仕様:1290行 4390行:実装コード 4580行:サポートコード	35人年 15ヶ月	自社開発のVDM派生言語	
1989-1991	原子炉自動停止システム(Darlington Nuclear Generator System)(原子力)	Ontario Hydro、AECL、AECB	高信頼性システムの開発、要求仕様の検証 規制機関への安全性説明	要求仕様、検証 6,000行:アセンブラ(SDS 1とSDS2全般). SDS1:7,000行、 SDS2:13,000行 (フォートラン)			
1988-1992	KVB,KVSKGV(自動列車保安装置)(鉄道)	SNCF GEC ALSTOM	安全システムの開発	仕様、実装、検証、 1993年以来6000車両以上に搭載、60,000行(B)、10,000証明責務、22,000行(Ada)		B	
1988-1989	TOKEN-BASED ACCESS CONTROL SYSTEM (TBACS)	NIST	暗号認証付スマートカードアクセス制御の仕様と検証、認証方式の改善、クリチカル機能の特定、検証	仕様、検証 300行(FDM)、2500行(C)		FDM (Formal Development Methodology, UNISYS)	
1986-1989	オシロスコープ(産業)	TEKTRONICS	オシロスコープ用、再利用可能なアプリケーションの開発	プロトタイプ設計 200KLOC		Z.、Fuzz (a type-checker)、Latex macros	

実応用プロジェクトリスト(続き)

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

開発開始時期(製品発表時期等から推定)	開発対象(ドメイン)	開発組織	適用効果等	適用範囲／規模	期間	適用形式、ツールチェーン	プロジェクトチーム、スキル
1982-1985	SACEM(鉄道信号と列車制御システム)(鉄道)	GEC Alsthom, MATRA Transport、RATP、CSEE	RATPの仕様に順ずる高信頼性システムの開発	設計、検証 検証コード:9,000行	120,000時間(形式手法工数)	B、Hoare Logic.	
1981-1993	Trafic Alert and Collision Avoidance Syatem (TCAS)(航空宇宙)	US Federation Authority	米国連邦航空局の命令により1993/12までにすべての航空機にTCASを搭載する	検証 7,000 lines of pseudo-code to describe the CAS Logic;		LaTeX、Pseudo	
1981-1991	CISS(顧客情報コントロールシステム)(エンタプライズ)	IBM	開発コスト:9%削減、エラー:60%削減、形式手法と従来プロセスの統合	要求仕様、設計、実装、検証		Z Method	
1981-1988	Multinet Gateway Systems(航空宇宙)	Ford Aerospace(Loral)	「U.S. Trusted Computer System Evaluation Criteria」の「developmental evaluation.」を得る	仕様、セキュリティモデル、セキュリティモデル:10頁 Gypsy MGS仕様:80頁、OS:6,000行		Rigorous mathematics Gypsy Verification Environment	
198x	Sizewell B(原子力)	TACS(英)		100,000行ソースコードの形式検証	約200人年	Malpas	

実応用プロジェクトリスト(続き)

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

開発開始時期(製品発表時期等から推定)	開発対象(ドメイン)	開発組織	適用効果等	適用範囲／規模	期間	適用形式、ツールチェーン	プロジェクトチーム、スキル
1998-	SPINLINE 3　制御コマンドシステム -Fessenheim & Bugey Power Plants(原子力)	Schneider Electric Framatome ANP Data systems & solutions	25行:Cコード確認/技術者/日 開発時間45%短縮 HWとの統合テスト65%短縮	1,200 SCADEモジュール:1,200 200,000行(C)自動生成		SCADE	
ー	原子力	KOPEC				SCADE	
ー	原子力	KAERI				SCADE	
ー	原子力	NPIC				SCADE	

実応用プロジェクト事例

防潮可動堤開閉意志決定システム／オランダ
航空管制システム：iFACT／イギリス
無人地下鉄車両の制御（パリ地下鉄14号線）
パリ地下鉄プラットフォームドアの制御
シャルルドゴール空港の無人シャトル制御
北京地下鉄の自動列車停止システム
Sao Paulo地下鉄プラットフォームドア
ニューヨーク地下鉄カナーシ線列車制御システム（CBTC）の最新化
Airbus社製航空機のシステム
艦載ヘリコプタ運行限界計装システム（SHOLIS）
コンポーネント仕様のモデル化（プジョー）
「Tokeneer ID Station (TIS) 」（バイオメトリクスID認証ツールのアクセス管理セキュリティソフトウェア）（NSA）

防潮可動堤開閉意志決定システム／オランダ(1/8)

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

- オランダの防潮可動橋管理システム(Storm Surge Barrier Control System)へ形式手法を適用

開発プロジェクトの概要	開発対象	オランダ運河のマエスラント防潮可動堤(水門)(Maeslantkering)の開閉意志決定システム(BOS)
	開発時期	BOS1:開発期間1995～1996年　1997年5月引渡し、1998年10月本格稼動(竣工) BOS2:2007年～2009年に、BOS1をアップグレード
	開発期間	BOS1:2年(12名体制、20人年) BOS2:1～1.5年(7名体制)
	開発規模	BOS1 ・SPINによる記述(プロセスアーキテクチャモデル、外部との通信モデル):N/A ・Z表記による記述(詳細仕様記述):29プログラム/20KLOC ・運用システムC++:200KLOC ・シミュレータ/テストシステムC++:250KLOC ・開発コスト:2.5～3百万ユーロ(ソフトウェア)、1百万ユーロ(ハードウェア) BOS2の詳細は不明だが、BOS1のモデルを再利用し再度詳細化
開発の背景	BOSは、暴風等による運河水位上昇・洪水防御のための水門(径360m)の開閉を完全に自律的に意思決定するシステムである。Rijkswaterstaat(State Department for the Maintenance of Ways and Waterworks 国家水路・水事業保全省)管轄のDeltaworksプロジェクトの一環で開発された。 第1次のBOS開発(BOS1)は、1995年に開始され、1998年に竣工した。その後ハードウェア(コンピュータ)が陳腐化し保守部品の供給の不安が生じたため、ハードウェアを刷新し、ソフトウェアの新規ハードウェアへのポーティングとソフトウェアの改善を2007年から2008年に実施した(BOS2)。 国家水路・水事業保全省の当初の要求仕様に形式手法を利用する要件があったわけではない。要求にあったのは、不具合を起こす可能性についてであった。これに対し、LogicaCMGは、IEC61508を適用する形式手法に基づくシステムの仕様を提案し、受注に成功した。以降に経緯を示す。 	

防潮可動堤開閉意志決定システム／オランダ(2/8)

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

- 形式手法を適用することで公開入札を落札し、プロジェクトを成功させる。

開発の経緯	1993-1994年	国家水路・水事業保全省からの要求に形式手法を使用する用件があったわけではない。要求にあったのは、不具合を起こす可能性についてであった。 これに対し、Logica社が国家水路・水事業保全省から仕様策定の業務を請負い機能仕様を作成した。 ※Logica社は1969年創立の英国ITベンダ
	1994年下期	公開入札プロセス：Den Hagg BVとLogica社が入札に応じ、 CMG Den Hagg BVは形式手法を採用することで、安全仕様を定義し、受注に成功した。 CMGが落札した理由は、安全系システムの標準であるIEC61508へ対応を明記したことと、Twente大学の協力を得て、形式手法ををを導入することを明記したころにあった。これにより、国家水路・水事業保全省に予定された予算枠で安全系システムを開発できる能力を説得することができた。 ※CMG社：通信業界に特化した1964年創立の英国ITベンダ、CMG Den Hagg BVはCMG社の公共セクタ部門
	1995～1996年	形式手法を採用し、BOS 1システムを開発（CMG社とLogica社）---12名の体制で2年、20人月
	1997年5月	第一次引渡し
	1998年10月	本格稼動開始（竣工）
	2002年12月	Logica社がCMG社と合併しLogicaCMGとなる。
	2007年	LogicaCMGは、通信部門を切離し、Logica社（英）に社名変更、通信部門は別会社、Acision社（英）となる。 ※Logica社では水門に関連する新規プロジェクトで形式手法を採用した開発を実施している（形式手法開発者を100名程度保持）。 ※Acsion社では通信システムの開発に形式手法を用いている。
	2007年11月	高潮の警報により始めて防潮堤が閉じられる。

防潮可動堤開閉意志決定システム／オランダ(3/8)

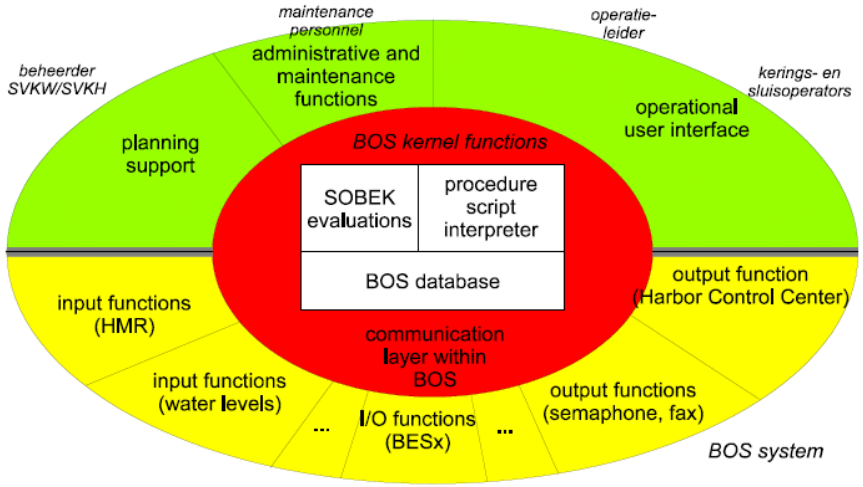
- その後、ハードウェア陳腐化等による安全性への懸念からシステムをアップグレード。その後、形式手法の技術はLogica社やAcision社に継承された

開発の経緯(続き)	2007年～	Logica社がアップグレードを受注しアップグレードを開始 旧式化したBOSシステム(BOS1)のハードウェアの交換 Stratus社フォールトトレラントコンピュータ(PA-RISC、FTX/HPUX)をStratus(X86プロセッサ、Linux)へアップグレード ハードウェアアップグレードに伴い、旧ソフトウェアを新規ハードウェアをポーティングするとともにモデルから再度詳細化を実施 BOS1プロジェクトと同様に、Z表記を用いた。仕様作成と設計はZ表記を利用してBOS1と同様のプロセスで行われた。妥当性検討(バリデーション)を必要とするアーキテクチャやプロトコルの変更はされないため、Promelaは使われていない。ハードウェア面には、単一のフォールトトレラントStratusコンピュータが採用された。通信ラインは標準の端末サーバに終端し、標準の冗長ネットワーキングにより、Stratusに接続された。新規のハードウェアの導入により総合的な障害の可能性が減少した。 ソフトウェアについては、下記のような改善がなされた。 1.外部環境のエラー検出を支援する診断プログラムの改善 2.GUIを実システムから切り離し、システムを簡素化し、比較的、非安全系のコンポーネントを別のハードウェアに移行 3.分析とデータマイニングを導入し、エラーのルートコーズ分析の決定を支援
	その後	Logica 100名弱の形式手法技術者がいると推定され、防潮可動堤開閉の意志決定システムの経験を活かした公共関連のプロジェクトを実行している。 しかしながら、SIL4 のプロジェクト開発に投資する顧客はまだ少ない。 形式手法の研究で Twente大学との研究を継続している。 Acision 通信関連製品の開発に防潮可動堤開閉の意思決定システム開発の経験を活かしている。 形式手法は、通信プロトコルの開発において必要度が高い。 インターネットRFCと3GPP仕様で形式表現が欠けている。 欧州研究プロジェクトの一部で形式アーキテクチャに関し Eindhoven工科大学と協力している。

防潮可動堤開閉意志決定システム／オランダ(4/8)

SEC
Software Engineering
for Mo･No･Zu･Ku･Ri

- 3名の形式手法専門家の支援を受け、5名のコアメンバと7名のソフトウェア技術者が開発

開発体制	Rijkswaterstaat(State Department for the Maintenance of Ways and Waterworks 国家水路・水事業保全省)の委託を請け、CMG Den Haag B.V.が開発 CMG Den Hagg BV:は1993年にLogica(創業40年のITベンダー)と合併、LogicaCMGとなる。 BOS2は、LOGICA社が受注 BOS1の開発体制(CMG Den Hagg BV) 5名のコアメンバが中心となり、3名の形式手法の専門家の支援を受け開発。他に7名のソフトウェアエンジニアが主にコーディングを担当 3名のFM専門家 Twente大学 CMG 5名のコアメンバ CMG 7名のソフトウェア エンジニア CMG  BOS2の開発体制(Logica) 7名の開発体制

防潮可動堤開閉意志決定システム／オランダ(5/8)

- SPINによる抽象モデル開発と妥当性検証、Zによる仕様作成、マニュアルで実行コード(C++)に変換

適用範囲・内容	SPINを用いたモデリングおよび検証(SPIN) プロセス・アーキテクチャおよび外部システムとの通信についてモデリングと検証 データとアルゴリズム解析(Zを使用) 機能および各プロセスにおけるデータのストアとフローについてモデリング 開発プロセス ■通信とインタラクションのモデリングと検証 プロセスアーキテクチャのモデル化/検証(Promela/SPIN) 外部システムとの通信のモデル化/検証(Promela/SPIN) コアアーキテクチャにデッドロック/ライブロックがないことを確認 *ビヘイビアのモデル化は比較的容易で有効だった。 *モデル検証により、プロトコルレベルの大きな変更がなされた。 ■データとアルゴリズムのZによるモデリング ケースツールを利用したBOSシステムのモデリング(Ward & Mellor) Zを利用し、ストアとフローの各プロセスの機能とデータのモデル化 スクリプトとLaTexによるツールケースからの設計ドキュメント生成 スクリプトツールにより、ケースツールからZタイプチェッカの入力が生成され、シンタックスが検証された。 *Zによるモデリングは難しく、習得に時間がかかった。 *テストケースとコード/設計レビューに有効であった。 *設計者、プログラマ、コードレビューアのコミュニケーションを支援するのに役立った(曖昧なコミュニケーションを防ぐ)。 ■実行(C++)コードの生成 マニュアルで行われた。

防潮可動堤開閉意志決定システム／オランダ(6/8)

SEC
Software Engineering
for Mo･No･Zu･Ku･Ri

- Promela／SPINに傾注する技術者がプロジェクトを牽引

ツールチェーン	■Promela/SPIN(Promela model describing control) SPINによる抽象モデル開発、アーキテクチャモデリングと妥当性検証、外部システムとの通信の妥当性検証 ■Ward & Mellor Case Tool、Zを用いたシステムのモデリング、機能および各プロセスにおけるデータのストアとフローについて、モデリング ■LaTex ドキュメンテーション
開発者のスキルレベル	コアとなった5名はいずれも経験8年以上ソフトウェア技術者であり、その内、3名は形式手法の経験者であった。特にKW氏は、Promela/SPINに傾注していた。 形式手法の経験のあるコアメンバを中心に、3名の形式手法専門家の支援を受け、形式手法のスキルを習得し、他のプロジェクトメンバに知識、経験を広めた。開発チームが必要なスキルを習得するために6ヶ月以上を要したという。 コアメンバの中でも、アーキテクチャはPromelaによるSPINのモデリング技術の経験があり、Zの読書きができる。プログラム担当者も同様である。コアメンバ以外に7名のソフトウェア技術者が、実行コード(C++)への変換やテストを実施したが、いずれもミドルクラス以上のソフトウェア技術者であり、プロジェクトにおいてZを習得した。C++ 実装やテストでは、Zを読むことは必要であったが、書くスキルは必要ではない。 ソフトウェア技術者の教育と継続的改善は必要であり、Zの習得は必要、ソフトウェア工学全般の教育強化が望まれる。 次ページにコアメンバと形式手法専門家の経歴、職種と形式技術者の簡単な経歴を示す。

防潮可動堤開閉意志決定システム／オランダ(7/8)

- ハイレベルのコアメンバ5名と7名のミドルレベルソフトウェア技術者が、Twente大学の3名の形式手法専門家の支援を受けて開発

開発者	開発時の所属	役割	現在の所属	経験	学歴
コアメンバ					
FB	CMG社公共部門先進技術	プロジェクトリーダ、プログラマ	Logica社, ソフトウェアエンジニアリング、システムアーキテクチャ研究グループ	電気工学修士、10年のプロジェクト経験	Delft工科大学
RR	CMG社公共部門先進技術	プログラム, システムエンジニア, コード/設計レビュー	Logica社, セントラル技術マネージャ、リードテクニカルアーキテクト	技術修士、10年の経験	Twente大学
KW	CMG社公共部門先進技術	アーキテクチャ/設計、品質	Acision社, 製品管理ディレクタ	電気工学修士／博士、8年+ の経験	Twente大学 (Electrical engineering)
RB	CMG社公共部門先進技術	プログラム	Tomtom社	修士(パラレルプロセッシング、トランスピュウータ、形式手法CSP/Z等7年の経験	Delft工科大学
WG	CMG社公共部門先進技術	テスト／分析	Logica社, Lead Expert Engineering /systems safety manager	博士(形式手法Zの専門家)	Vrije大学Amsterdam Utrecht大学
形式手法専門家					
JT	Twente大学,コンピュータサイエンス形式手法、ツール研究グループ	形式手法専門家	ESI リサーチフェロー エンベデッドシステム協会リサーチフェロー Nijmegen大学準教授	博士	Twente大学電気工学、コンピュータサイエンス
PK	Twente大学コンピュータサイエンス学科テレインフォメーション＆オープンシステム部門形式手法グループ	形式手法専門家 (SPIN)		博士	
MC	CMG社公共部門先進技術	形式手法専門家	Eindhoven工科大学	博士	Leiden大学CS(1987-1992) T Hoare教授の下、Oxford大学プログラミング研究室で修士を得る(1990-1991)

防潮可動堤開閉意志決定システム／オランダ(8/8)

SEC
Software Engineering
for Mo･No･Zu･Ku･Ri

- ソフトウェアに重大なバグは発見されなかった

開発成果	■ソフトウェアに重大な欠陥は発見されず、ソフトウェア品質に問題がないことが確認された。 ■Zを用いたモデリングを経験： テスト実施者やレビュー実施者はテスト・ケース作成やコード・設計のレビューを効率的に行えるようになった。 ■各工程間のコミュニケーション促進・曖昧さを解消に役立った。 （設計者、プログラマ、テスト実施者・コードレビュー実施者、保守作業における人的要素を過小評価をしないこと） ■ソフトウェア設計は元より、HWやパーツの寿命を勘案した保守活動全般が重要であり、留意すべきことがわかった。 ■仕様記述・モデルテスト・コードレビューが連携した。 ■IEC61508、SIL4対応に対応できた。 将来に向けての教訓 仕様作成、設計工程の支援. 1.ほとんどの問題は、仕様と設計の段階に起こる。実装段階ではない。. 2.外部システムも形式仕様に含む必要がある。 3.実用的なメソドロジとツールのサポートが形式手法の採用を容易にする。 4.技術者を支援する形式手法表記とツールの必要性（Verum、Esterel、ClearSy等のツール） コンピュータサイエンス教育で学ぶ標準的形式手法メソッドをベストオブブリードで定めていくこと 1.どのように仕様を定義するかを学ぶことが重要な技術的知見 2.形式手法には、あまりにも多くの種類がある。

航空管制システム：iFACT／イギリス(1/2)

SEC
Software Engineering
for Mo･No･Zu･Ku･Ri

- ZとSPARKによる航空管制システムの開発

開発プロジェクトの概要	開発対象	航空管制システム/iFACTS(interim Future Area Control Tools Support)
	開発時期	2005～2007年　その後も継続中
	開発期間	一部の作業は現在も継続されており、明確に期間を定義できない。
	開発規模	Z仕様2,000頁超・SPARKとAdaによる25万行以上、総費用50百万ポンド(約70億円、1ポンド=140円換算)
開発の背景	英国政府では、旅客者数が2020年までに現在の2倍、30年までに同3倍へ急増すると試算 2013年までに年間フライト数3百万本へ対応(現2.3百万本) 新技術を採用した管制システムの導入、管制官への旅客機航行支援、安全性の確保が不可欠と判断 レーダーシステム有史来最大・革命的な航空管制(ATC)システム 事故予測、コンフリクト検出、航路モニタ 航空管制システムとしては、世界で最先端 航空機が航行計画に従わず航路を外れた場合、管制官に対し事前に警告を発し、衝突回避等のための判断情報を提供する。 完全な電子データによる管理、洗練された複数ディスプレイ・モニター 	

航空管制システム：iFACT／イギリス(2/2)

SEC
Software Engineering
for Mo･No･Zu･Ku･Ri

- 必要な技術スキルは、Aランク20%、Bランク30%、Cランク50%

開発体制	ユーザ：NATS（National Air Traffic Services）、PraxisとNATSのジョイントプロジェクト 場所：Hampshire Swanwickロンドン地区管制センター Praxis：仕様記述、ATSシステムソフトウェアの開発、NATS開発者のトレーニング、Praxis受注額10百万ポンド（同、約14億円） 他ベンダー：Lockheed Martin、IBM、AdaCore、など 機能仕様の段階では約12名の技術者が関わった。実装、テストの段階では、約150名の技術者が関わっている。 管制管理システムは、特殊なシステムであり、システムの経験と理解があるユーザ（NATS）の関与が欠かせない。プロジェクトには、NATSの開発者が各段階で半数程度参加している。
適用範囲・内容	機能仕様記述、ATSシステムソフトウェアの開発 既存のNERCシステムに付加し、仕様記述と実装を実施 従って形式手法の適用範囲は、機能仕様記述（Z）、コーディング（SPARKが90%）とテスト、検証となる。
ツールチェーン	SPARK AdaCore Z Fuzz (Oxford 大学)：シンタックスエラー、タイプエラーの検出
開発者のスキルレベル	電子技術者、システム技術者、数学的素養がある技術者など様々な背景の技術者からなる。数学的素養のある開発者の不足が指摘されている。 技術者のランクを3段階とすると、一般的に、 A ランク（実装技術だけでなく、特定分野の専門スキルや管理能力を有す）の技術者：20%、 Bランクの技術者（Zの記述と読込みができる：30%、 Cランク（Zの読込みはできるが記述はできない）の技術者：50%の構成となる。 形式手法、あるいは安全に関するスキルと経験のある技術者の単価は、一般のソフトウェア技術者の1.2倍程度となる。
開発成果	不具合の大幅な削減（具体的な数値は公表していない） 信頼性の高いシステムの実現（具体的な数値は公表していない） 生産性についての公表はしていないが、一般的なこととして、形式手法の採用により、信頼性は向上するが、生産性の向上は見込まれない（同等、もしくは悪くなる）。

無人地下鉄車両の制御(パリ地下鉄14号線)(1/2)

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

- STS(Siemens Transport System)がBを採用して開発した初めての鉄道車両制御システム

開発プロジェクトの概要	開発対象	無人地下鉄車両の制御(パリ地下鉄14号線)(RATP;パリ交通局)
	開発時期	1994-1998
	開発期間	4年　Bメソッドを採用した初めてのプロジェクトであったため4年の期間を要した。
	開発規模	86,000行(ADA)、115,000行(Bライン)、27,300 (数学的証明数;mathematical Proofs)
開発の背景	フランス政府は1989年にプロジェクトを開始し、地下トンネル工事は1993から1995年にわたり行われ、1998年に自動運転を開始した。 パリ地下鉄14号線 路線長:8Km 駅数:8 車両間隔:115秒 速度:40Km/h 車両数:17 乗客数:350,000／日 開発は、「Matra社」が行った(Siemens社は、Matra 社を買収し、現在Siemens Transport Systems(独Siemens傘下の仏企業)となっている)。 SAET L14:Système Automatique d'Exploitation des Trains L14 地下鉄14号線は、完全自動システムであるため、安全系システムには、列車の発車と停止、列車のドアとプラットフォームドアの開閉に係わるシステムがある。プログラムは3つのサブシステムに分解される。 1.軌道設備(軌道に沿って複数設置) 2.車載機器(各列車に1インスタンス) 3.ライン機器(1インスタンス) 各サブシステムは相互に接続されている。 各サブシステムの安全系はB表記を利用して開発された。 中央の列車指令システムはDEC Alpha上のOpenVMSで動作 車載システムはDIGISAFEと呼ばれる3つのマイクロプロセッサMC68020上でMRTK(Matra Real Time Kernel)と呼ばれる専用ソフトウェアが動作	

無人地下鉄車両の制御(パリ地下鉄14号線)(2/2)

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

- STS35名、RATP15名、期間4年間の時間と工数を必要とした

開発体制	RATP 15名(仕様、妥当性検証) STS 35名(モデル開発、コード生成、検証、テスト)
適用範囲・内容	仕様記述 自動コード生成 検証 妥当性検討
ツールチェーン	Atelier B/ClearSy Ada Core
開発者のスキルレベル	STS 10年以上の経験者:3名(1名PHD、他2名はSWエンジニア)がプロジェクト管理とプロセス管理を実施 10年以下の経験者:32名がモデリング、検証、コード生成、テスト、妥当性検証を実施 当初はSWエンジニアとして入社するが、社内研修を経て、形式手法のスキル(Bの記述の読解を習得する。 RATP シニアとジュニアのSWエンジニア:15名(仕様作成、妥当性検討を実施)、Bを記述するスキルは必要ない。妥当性検証のために読込むスキルが必要
開発成果	1998年に自動運転を開始した無人運転システムであり、車載制御システムを搭載する列車と、搭載しないシステムを同時運行できる。Bメソッドが利用された初めてのアプリケーションとして成功した。すべての不具合は開発プロセスで発見され、妥当性検証は単体テストをすることなく、効率的に実施できた。 システムの安全系はB手法を用いて確認された。証明(Proof)の後、機能検証、統合検証、オンサイトテスト、運用においてバグは発見されていない。 Bメソッドを利用した初めてのプロジェクトであったため、STS(旧MATRA)の技術者35名、RATPの技術者15名という多数の技術者とシステム全体で4年の開発年月を要した。ここでの成果が以降の類似プロジェクトの基盤となった。

パリ地下鉄プラットフォームドアの制御(1/3)

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

- Bを利用した地下鉄プラットフォームドア制御システムの開発をClearSyが担当

開発プロジェクトの概要	開発対象	パリ地下鉄 プラットフォームドアの制御(コマンドコントローラ/COPPILOT)(RATP;パリ交通局)
	開発時期	2006年
	開発期間	9ヶ月 (EventBモデル、3ヶ月)
	開発規模	形式手法 B モデル 3,500行(証明数:1000. 90%自動証明)
開発の背景	フランスのRATP(パリ市交通局)ではプラットフォームドア(PSD)により、乗客が線路内に入込んだり、転落することを防ぐシステムを無人地下鉄運行に採用している。新開発のPSDの全路線導入に先立ち、パリ地下鉄13号線の3駅においてプロトタイプPSDの開発プロジェクトを立ち上げた。車両の到着、停車、発車を車両との直接の交信をすることなしに検出するコマンドコントローラ/COPPILOT(SIL3準拠)の開発は、ClearSy社が担当した。 コマンドコントローラは、車両のドアの開閉状態を検知し、PSDにドアの開閉命令を出す。開閉命令の障害は乗客の怪我や生死につながるため、車両の規格(EN50126, 50128, 50129 など)に従って設計、テスト、検証された。 Bメソッド採用の背景 要求安全レベル、信頼性とトレーサビリティの達成を限られた開発期間で達成するために、開発の各工程での検証の工数を削減する必要があった。このために、Bメソッドが、ほとんどのプロジェクトフェーズで使われた。 
開発体制	RATP:人数不明(要求仕様、仕様作成、検証、妥当性検証) ClearSy:4名(プロジェクトマネージャ、開発技術者、安全技術者、検証技術者)(仕様作、モデル開発、コード生成、検証、テスト、妥当性検証) KABA:プラットフォームドアの供給

パリ地下鉄プラットフォームドアの制御(2/3)

SEC
Software Engineering
for Mo･No･Zu･Ku･Ri

- システム仕様を調整し、9ヶ月の短期開発を実現

適用範囲・内容	■機能分析での形式手法適用 RATPは開発実行前にシステムの形式機能分析を行い、SOW(statement of work)の完全性と曖昧自由度を評価した。 プラットフォーム上に設置される2つのレーザテレメータ(遠隔測定機)による二次元画像認識を採用し、車両の到着、出発と同時に車両ドアの開閉を検知する方法をBメソッドを利用し開発、システム(PSD＋コントローラ)全般の検証、機能の制約と安全属性を検証した。 2つの独立した(しかし調和していない)画像認識アルゴリズムは、プロジェクトの開発期間を考えると危険と判断され、最終的に採用されなかった。 厳しい開発期間の制約のため、センサ技術への依存が密でないセキュアなアーキテクチャを採用し、規格審査機関の迅速な認定を得られるようにした。このアーキテクチャでは、SIL3標準のSiemensセーフティオートメーション(Siemens S7 PLC)と通常の赤外線とレーダセンサを採用した。 ■システム開発における形式手法適用 1. 機能分析で得られたモデルが再利用され、新たなアーキテクチャが、フランスの地下鉄の規制の一部を含むシステムの機能仕様に従う証明(Proof)がなされた。 システム仕様とソフトウェア仕様が、Bにより形式化され、コントローラ機能は、精密にモデル化された(車両到着、車両検出、車両出発、車両ドアの開閉等)。その間に、同時進行でセキュリティチームによりセーフティケースが開発され、外部要因がどのようにPSDコントローラのふるまいに影響を及ぼすかが定義された。 2. Bモデルは、 Brama animator によりアニメーション化され、与えられたシナリオで検証された。モデルのアニメーション化は、SIL3 ソフトウェアの認証に必要な検証プロセスではないが、モデルのチェック、適切性の内部検証に役立った。 3. システムレベルモデルから部分的に仕様が詳細化された。この際にComposysツールを利用し、Bモデルに文脈情報(コメント、記述、コンポーメント名等)を付加することで、自然言語でシステムを完全に記述する仕様書類を生成した。この書類は、形式モデルを読んだり理解できないドメインの専門家とモデルを確認するために使われた。 4. ソフトウェアは、Bで記述され、仕様に従っていることが証明された(LADDER言語での記述も可能だが、SIL3 の認証のためには、グラフィカルインタフェースによるソースコードの入力が必要となる)。 5. Bは、専用のトランスレーションスキーマによりLADDERへ変換された。BからLADDERへのステートダイアグラムの変換は比較的単純であり、最適化が行われ制約(特にサイクルタイム)条件の検証がなされた。

パリ地下鉄プラットフォームドアの制御(3/3)

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

- プロジェクトマネージャ、安全技術者、開発技術者、検証技術者の4名の体制で開発

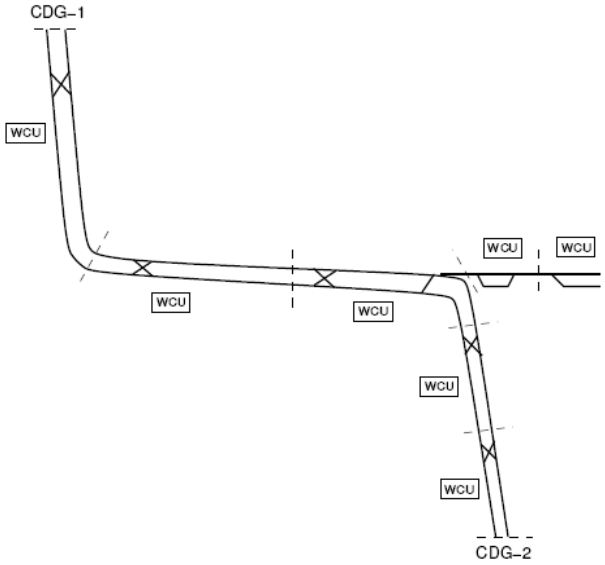
ツールチェーン	COMPOSYS(分散システム向けBモデリングツール、Bモデルからのドキュメント生成ツール) B4Freeフリーソフト(Bモデルの証明:B メソッドのための統合支援ツールであり、編集系、型チェッカ、証明責務、生成系、証明支援系を含む) Atelier B(Bモデルの証明) Brama Animator
開発者のスキルレベル	ClearSy プロジェクトマネージャ:経験年数5年以下のソフトウェアエンジニア1名 安全技術者:シニアソフトウェアエンジニア1名 開発技術者:ジュニアソフトウェア技術者1名 検証技術者:ジュニアソフトウェア技術者1名
開発成果	SIL3取得 初期システムレベル機能仕様:130ページ セーフティケース:300ページ 開発ドキュメント:600ページ 形式手法 B モデル 3,500行(証明数:1000、90%自動証明)

シャルルドゴール空港の無人シャトル制御(1/4)

SEC
Software Engineering
for Mo･No･Zu･Ku･Ri

- 無人(Driverless)シャトルの制御をするWCU(Wayside Control Unit)の開発

開発プロジェクトの概要	開発対象	シャルルドゴール空港の無人シャトル制御(Roissy WCU-SCS project)
	開発時期	2006年
	開発期間	N/A
	開発規模	ソフトウェア機能仕様書:228ページ Bモデル:183,987行 ADA:158612行 証明数:43,610
開発の背景	シャルルドゴール空港のシャトルシステムは、シカゴのオヘア空港のシャトルから派生したシステムである。オヘア空港のシャトルと違い、軌道に沿って高度にコンピュータ化された「Wayside Control Unit」(WCU)と呼ばれる制御ユニットが複数設置されている。各制御ユニットは、イーサネットで接続されており、予め設定された速度の運行プログラムを送り各車両を制御する。車両は、軌道と「Wayside Control Unit」に設置されたセンサが検出した状態に応じて制御される。 ソフトウェア仕様は、オヘア空港のシャトルの仕様書類を利用し、形式化された。	



シャルルドゴール空港の無人シャトル制御(2/4)

SEC
Software Engineering
for Mo･No･Zu･Ku･Ri

- シカゴオヘア空港のシャトル制御の開発ドキュメントを利用し開発された。

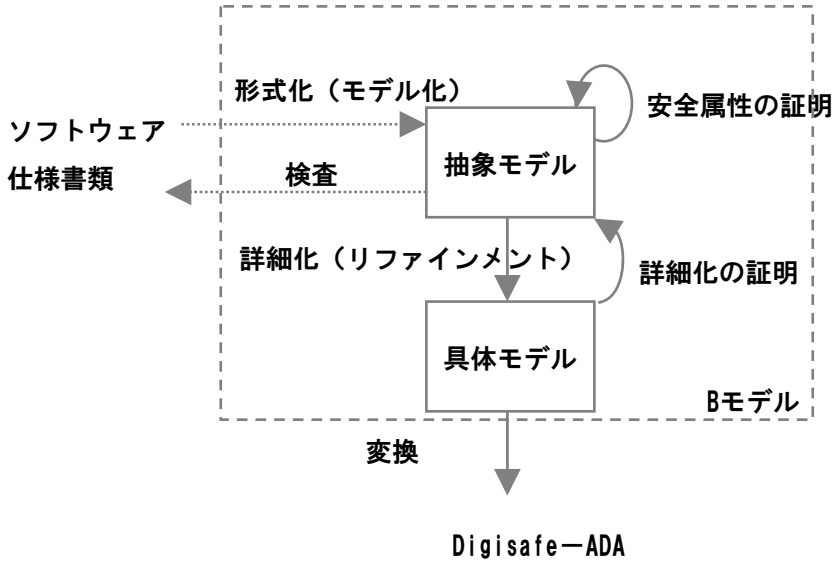
開発体制	ADP(Paris Airport) Siemens Transportation Systems(STS) ClearSy(Bモデルの開発)
適用範囲・内容	B手法でモデル記述、詳細化、検証を行い、ADAコードを自動生成した。 安全系ソフトウェアの部分(WCU-SCS)はBで設計され、Ada(Digisafe Ada)に変換された。 開発プロセスを下記に示す。 1. システムの仕様は、形式手法が適用されていない過去の複数の設計書類を利用して策定された。シカゴのオヘヤ空港のVALの設計書類(B手法がSimenseで採用される前の10年目に開発された)の3主要モジュール(ブロックロジック、ルートロジック、モードロジック)の仕様が利用された。 2. 仕様(200ページ)をBの抽象モデルへ変換する作業はClearSyが行った。 変換プロセスのエラーを最小限にするため、ソフトウェア仕様に関する「質問と回答データベース」を採用し、ClearSy社の質問がSTSにより回答されるプロセスをトレースするようにした。STSは必要に応じ、ClearSyに詳細な説明を行う。この仕組みはClearSy社が仕様を理解するために重要なプロセスとなった。 3. このプロセスで仕様書類の修正と調整が行われ、定期的に仕様が更新された。 4. Bの抽象モデルを自然言語の仕様と対比し確認をするために、B記述を担当していないモデリングチームによる検査チームが置かれた。検査チームは、Bの抽象モデルが、仕様書類と対比して正確であることの確認をした。 5. 検査において疑問や質問が生じた場合には、Bモデルが変更されるか、「質問と回答データベース」にフォワードされる。 B抽象モデルと仕様のトレーサビリティは、各抽象オペレーションの最初の部分で、品質保証コメントとして明確なリファレンスとともに示される。 6. 自動詳細化(リファイメント)の前に、手動で詳細化(リファインメント)の準備がされた。このステップで、開始点の抽象マシーンを小さな抽象マシーンに分割し、詳細化のオペレーションを簡易化するための中間詳細レベルを記述することで、自動詳細化の複雑さを軽減する。

シャルルドゴール空港の無人シャトル制御(3/4)

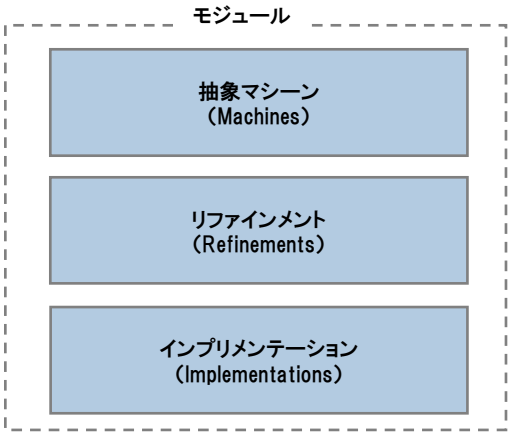
SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

- 詳細化(リファインメント)では、STSの内製ツールが利用された。

適用範囲・内容(続き)	7. 次のステップでは、自動詳細化ツールを使い詳細化を行う。 EDIth Bと呼ばれる内製ツールが利用され、抽象マシーンとリファインメントからインプリメンテーションを生成すると同時に、新たなにサブ抽象マシーンを生成する。 Bertilleは、サブ抽象マシーンをルールベースを利用し、さらに詳細化する。このプロセスが具体モデルが生成されるか、詳細化が失敗するまで行われる。 8. 生成された具体モデルの静的チェックと証明が実行される。 9. 証明されたBモデルからADAコードを生成する。



参考:Bモデルの構造



■Bモデルはモジュールにより構成され、データとデータの操作を行う。モジュールは、抽象マシーン、リファイメント、インプリメンテーションから構成される。

■マシーンはモジュールの外観を示す。

■リファインメントはモジュールの内観を示し、モジュールのふるまいを定義する。

■マシーンとリファイメントは抽象コンポーネント(抽象モデル)である。

■インプリメンテーションは、より具体的な記述であり、従来の言語に直接変換可能である。データ構造は限られている(整数、ブーリアン、配列)。

シャルルドゴール空港の無人シャトル制御(4/4)

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

- **抽象モデル開発の費用が55%、詳細化(リファインメント)の費用はツール導入により24%となった。**

ツールチェーン	EDiThB (半自動仕様詳細化ツール、マシーンとリファインメントからインプリメンテーションを実装するSTSで開発された内製ツール) Bertille (半自動仕様詳細化ツール、具体モデルまでの詳細化を支援するSTSで開発された内製ツール) Atelier B(自動証明、ClearSy社)
開発者のスキルレベル	仕様書からBの抽象モデルを開発するには、Bの読解だけでなく、記述能力とさらには仕様書を理解するためのドメインの知識が要求される。 詳細化のモデルはツールを導入することで負荷が低減したが、複雑なプロセスであり、Bの読解と記述能力、最終言語(ADA)の理解が必要となる。
開発成果	開発されたソフトウェアはIEC61508: EN50126、EN50128、EN50129に準拠し、 SIL4に分類された。 ADAに変換されたツールは、従来プロセスで手動で開発されたコードより10%程度遅くなった。これは詳細化(リファイメントルール)によるものであり、最終的に詳細化のルールを修正することで対応した。 構築されあBモデルは、約183,987行、このうち抽象モデルが28,163で全体の約15%(マニュアルで作成)であり、詳細化により自動で作成された具体モデルが、約128,000行(70%)であった。 全体で43,000 程度の証明課題が存在し、このうち1,400 程度(3%)がマニュアルでインタラクティブに証明され、その他は、Atelier B により自動証明をすることができた。ADAの実行コード数は、158,612行となった。 工数の費用比率を下記に示す。

準備	5%
プロジェクトマネジメント	8%
抽象モデル開発	55%
モデル開発	[16%]
Q&Aと書類分析	[18%]
検査	[5%]
証明	[16%]
具体モデル開発 (詳細化)	24%
具体モデル作成	[13%]
証明	[11%]
最終化 (構成管理、書類化等)	8%

北京地下鉄の自動列車停止システム

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

- ClearSy社がAlstom社からソフトウェア開発を受注し実装した。

開発プロジェクトの概要	開発対象	北京地下鉄線の自動列車停止システム（Automatic Train Protection）（Urbalis Evolution Project）
	開発時期	2006～2008
	開発期間	1年8ヶ月
	開発規模	N/A
開発の背景	北京オリンピックに備え整備を進めた、北京地下鉄線の安全系ソフトウェア（CBTC）の開発にBメソッドが適用された。システムのモデル化とモデルBメソッドを用いたSIL4の形式証明が実施された。 およそ2年間にわたり、ClearSyとAlsthomは北京の地下鉄の安全系ソフトウェアの開発に携わった。 ClearSyの技術者が、Alsthomをサポートし、車載の安全系ソフトウェア（Automatic Train Potection）を開発した。ソフトウェアの主な機能は、軌道上の列車を検知し、安全の条件が満たされない場合に非常ブレーキを動作させることにある。 
開発体制	ClearSy、Alsthom 仕様設計の段階Alstomのチームがすべての機能を形式化した。この仕様を元にClearSyの技術者が、Alstomのチームと連係し、Bメソッドを適用し、仕様を形式化し、微調整した後、最終的にAdaに変換した。	
適用範囲・内容	仕様設計、実装	
ツールチェーン	Atelier B、AdaCore	

Sao Paulo地下鉄プラットフォームドア(1/2)

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

- 韓国POSCON社が、Sao Paulo地下鉄のプラットフォームドアを受注

開発プロジェクトの概要	開発対象	PSD(プラットフォームドア)
	開発時期	2009年3月～ 2010年12月
	開発期間	システム開発:12ヶ月、ソフトウェアの開発(機能仕様、コード生成、検証):3ヶ月
	開発規模	10,000 LOC(自動生成)
開発の背景	TRENDS社からPSDシステム(ブラジルのSao Paulo地下鉄 2号線、4号線のPSD(プラットフォームドア)を受注 1.「RAMS SIL-3」の認証の取得を要求された。 2. 開発期間2009年3月から2010年までの12月の12ヶ月間と短期間であった。 目標 「RAMS SIL-3」に基づき信頼性と可用性を保証すること。 1. 信頼性 99.95%,、可用性 99.998% 2. システムの信頼性と効率を改善すること 3. 製品価値を向上すすことで運用コストを削減すること 4. PSDシステムの安全性を保証すること ブラジルのSao Pauloの地下鉄システムにおいて「RAMS SIL-3」を達成することが要求された。 その他の鉄道システムにおいても、RAMSの適用が入札の条件となっている。 PSDの事業計画 1. ブラジルSao PauloのPSDプロジェクトで事業を開始する。 2. 多くの海外企業からのPSDシステム事業での協業要求を事業化する 3. 中国、台湾、アゼルバイジャン、カザフスタン、南米(ブラジル、アルゼンチン、チリ等)で、PSD供給の交渉中 安全への要求 1. 安全システムに関連するソフトウェアでは、フェイルセーフのコンセプトの下に、機能安全国際標準IEC61508のSIL3が要求される。 2. 国際標準EN50128を考慮しなければならない。 開発されるソフトウェアは、EN50128が推奨するオープンシステムのコンセプトを考慮し、ポータビリティ、相互運用、接続性の標準に従う必要がある。	

Sao Paulo地下鉄プラットフォームドア(2/2)

SEC
Software Engineering
for Mo･No･Zu･Ku･Ri

- SCADEを導入することで、3ヶ月間の短納期を実現した。

開発体制	韓国POSCOグループのグループ企業であるPOSCON社の3名の開発者による開発 顧客：TRENDS ENGENHARIA E TECNOLOGIA LTDA & Brazil Sao Paulo METRO
適用範囲・内容	機能仕様、モデル作成、コード生成、検証
ツールチェーン	SCADE
開発者のスキルレベル	開発者はソフトウェア工学の学位を持つが、特に数学的知見や形式手法の地域を有する開発者ではなかった。
開発成果	短期間(3ヶ月)に、仕様の開発、モデル開発、コードの自動生成(約10,000行)を実現した。 現在(2009年10月)、クライアントによるバリデーションを実施中。 プロジェクトの開発期限は非常に短く、SIL3認定のために、ソフトウェアのソースコード開発を含むV&Vの開発プロセスを必要とした。 SCADEは、Cコード生成でSIL3、4の認定を支援する唯一のツールであった。 SCADEのモデリング機能により、仕様からコーディングまでの機能的アプローチを提供することで、短期の開発期間に間に合わすことができた。 *当初は、Bメソッドの利用を検討したが、形式手法やツールの習得に時間がかかることが予測されたため、比較的導入が容易であるSCADEを採用することになった。

ニューヨーク地下鉄カナーシ線列車制御システム(CBTC)の最新化(1/3)

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

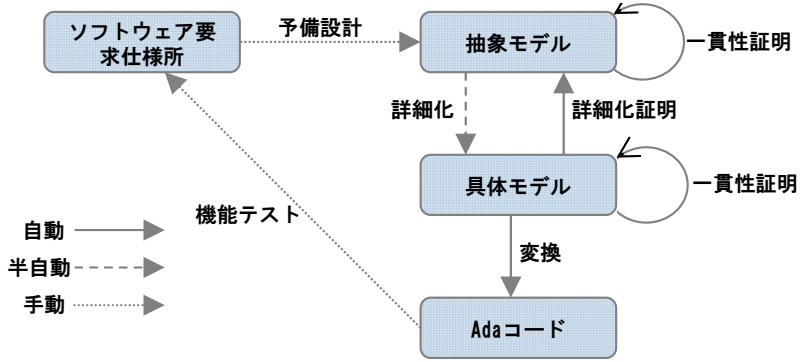
- パリ地下鉄14号線の経験と技術の蓄積を利用し、CBTCを開発

開発プロジェクトの概要	開発対象	列車制御システムの最新化　無線による無線制御システム(CBTC)
	開発時期	2001～2005　2006年(就業開始)
	開発期間	5年　133百万ドル
	開発規模	110,000行(Bライン、自動生成)、82,500(証明責務)
開発の背景	ニューヨーク市都市交通(NYCT)は、信号システムを、固定ブロック、軌道信号／トリップストップ技術から、無線による列車制御(CBTC)技術へ最新化した。STS(Semens Transportation System)社は、このプロジェクトを135百万ドルで受注した。 STS社は、Bメソッドを採用し、CBTCを開発した。STSがBを採用した最初の大規模プロジェクトはパリ地下鉄14号線であった。Bを利用することで、簡潔で曖昧性のない、ハイレベルのソフトウェア仕様(抽象モデル)を、ローレベルのコードのアルゴリズム(実行コード)と分離することができる。これにより妥当性検証チームは、詳細コードの開発に時間をとられることなく、仕様の開発に集中できる。 ニューヨークカナーシ線のCBTC開発では、パリ地下鉄の無人地下鉄の制御システムやその後のSan Juan や香港の地下鉄でのSACEM開発で技術を蓄積したBメソッドとAtelier Bツールを利用した開発プロセスを採用した。カナーシ線のCBTCプロジェクトではさらに、詳細化(リファインメント)のプロセスに新たなツール(Edith B)を導入することで開発プロセスを効率化した。 マイルストーン 2001年7月　予備設計レビュー 2002年3月　予備相互運用インタフェース仕様の準備 2003年7月　最終設計レビュー、初期ソフトウェアバージョン 2003年10月　初期CBTCテスト開始 2003年11月　車載機器設置開始 2005年3月　全車両設置、運用準備完了 2005年9月　シャドーモード(Rockaway to Livonia) 2005年10月　初期セクションCBTC運用 2006年春　全線でCBTC運用開始	

ニューヨーク地下鉄カナーシ線列車制御システム(CBTC)の最新化(2/3)

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

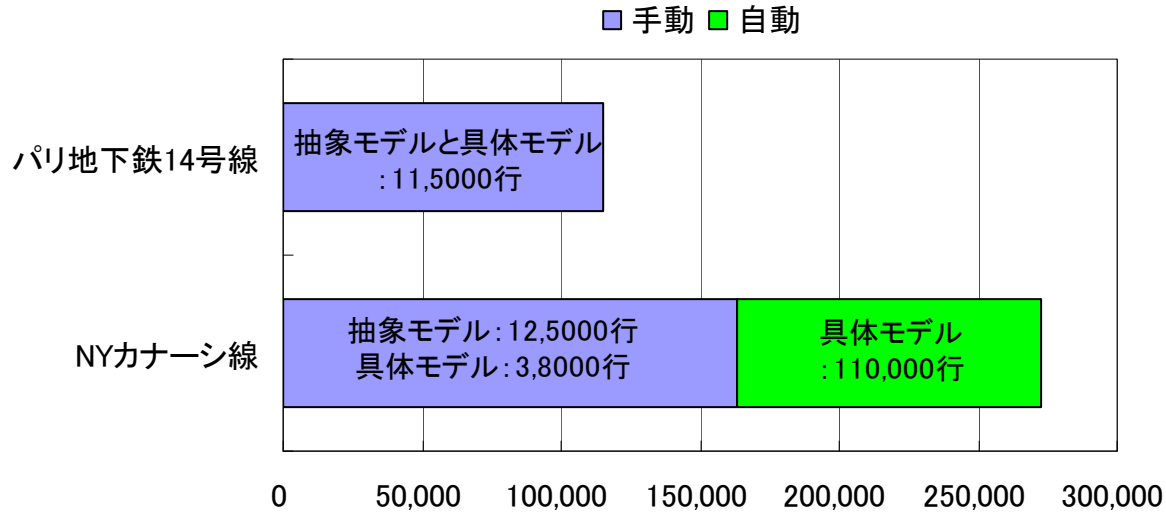
- 詳細化の工程にツールを導入し、半自動で詳細化(リファインメント)を実行

開発体制	ニューヨーク市都市交通(NYCT)がSTSへ開発依頼 車載ソフトウェアは4名のチームにより、約1年の期間で開発された。
適用範囲・内容	CBTCの開発は、STS社の内製ツールである半自動詳細化ツール EdithBを利用し、詳細化の工程を半自動化することで開発効率を改善した。  CBTCシステムは、STS(Semens Transportation System)「DIGISAFE XME」プラットフォームを利用している。 「DIGISAFE XME」は、数値計算の安全性をハードウェアの冗長ではない、「Vital Coding」技術によるコーディング(情報冗長)により実現する。 「DIGISAFE XME」のNYCTによる承認と、関連する機関による認可のために、Battelle社とアセッサ契約を結び、Battelle社がTÜV InterTrafficと再契約した。 DIGISAFEプラットフォームは、パリ地下鉄14号線に使われた新世代の高信頼性コンピュータである。 TÜV InterTrafficの役割 DIGISAFE XMEプラットフォームのセーフティアセスメントは、EN50128 SIL4システム鉄道標準に従った。 ーセーフティ対策が考慮されている、関連する標準のセーフティ要求に合致しているかの検証 ー危険を減らすために実装された対策が効果的であるかの判断 ーカナーシ線の沿軌道設備と車載設備への「DIGISAFE XME」プラットフォームの実装におけるセーフティアセスメントへの参加 車両は日本の川崎重工業製 

ニューヨーク地下鉄カナーシ線列車制御システム(CBTC)の最新化(3/3)

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

- 半自動の詳細化(リファインメント)ツールの導入により開発効率が大幅に改善した。

ツールチェーン	Atelier B AdaCore EDiThB(STSで開発された内製ツール／半自動詳細化ツール)
開発者のスキルレベル	車載ソフトウェアは4名のチームにより、約1年の期間で開発された。4名のうちパリ地下鉄14号線での開発経験があるのは2名であり、他の2名は、Bによる開発経験はない(1名はBの理論について知識があった)。形式手法の専門家は必要としなかった。 工程　技術者数　平均工数　パリ14号線の経験者数 ソフトウェア仕様形式化　4名　7ヶ月　1名 詳細化　3名　3ヶ月 証明　3名　3ヶ月　1名 機能テスト　3名　3ヶ月
開発成果	詳細化ツールの導入により、パリ地下鉄14号線と比較し大幅に開発効率が向上した。パリ14号線の開発規模に比べ、B表記の行数で約2.5倍になっているにも係わらず、開発期間は約1年と短く、投入人数も4名となっている。 

Airbus社製航空機のシステム(1/4)

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

- AirBus社で主なシステムの開発にSCADEを利用している。

<table>
<tr><td rowspan="4">開発プロジェクトの概要</td><td>開発対象</td><td>Airbus社の航空機(A340-500/600、A380)
フライトコントロールシステム、フライト警告システム、電気負荷管理システム、アンチアイシングシステム(防氷)、ブレーキとステアリングシステム、コックピットのディスプレイシステム、ATSUの一部(機体／管制基地通信)、FADEC(エンジン制御)、GUIコックピットの仕様書</td></tr>
<tr><td>開発時期</td><td>1990年代後半～2005</td></tr>
<tr><td>開発期間</td><td>N/A</td></tr>
<tr><td>開発規模</td><td>785,000行(自動生成 C言語ソースコード)(フライトコントロールガイダンスユニット開発の例)</td></tr>
<tr><td>開発の背景</td><td colspan="2">Airbus社ではESTEREL社のSCADEを使用し、A340-500/600シリーズ(2002年から8月就航)向けシステムの開発をしている。システムはDO-178B(航空無線技術委員会(RTCA)によって作られた、米国における航空用ソフトウェアの開発用ガイドライン)に対応する。
A380とA400Mのコックピットコントロール、ディスプレイシステム、オンボード空港ナビゲーションシステムディスプレイのグラフィックインタフェースは、SCADE Displayを利用し開発された。
■開発対象
Airbus A340(A500/600、A380)
Flight Control System
Fly-by-Wire-Controls
Display Computer
Warning & Main Computer
■フライトコントロールガイダンスユニット開発の例
3000SCADEシートを導入し開発
15000以上のI/Oが1msのレスポンスタイムで動作
785,000行のC言語ソースコードが自動生成された。
■各システムのLOCのうち自動コード生成されたLOCの割合
70%:Flight Control System
70%:Fly-by-Wire-Controls
50%:Display Computer
40%:Warning & Main Computer
  </td></tr>
</table>

Airbus社製航空機のシステム(2/4)

- サブコンポーネントの2/3はサプライヤによる社外開発

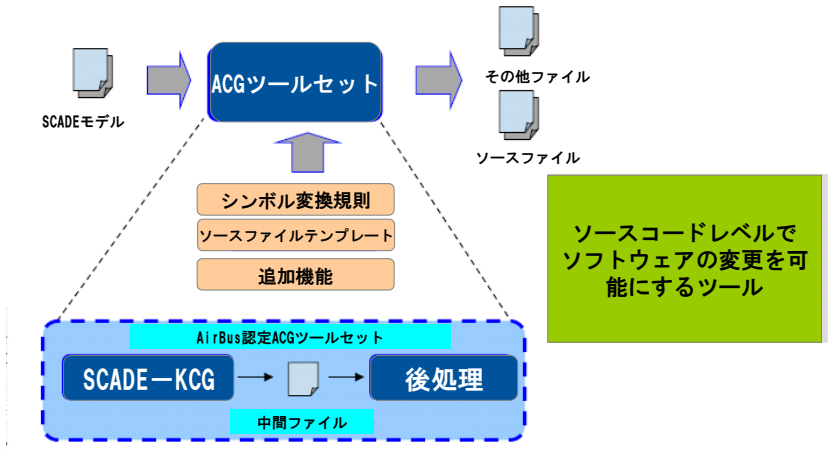
開発体制	サブコンポーネントの内 1/3は自社開発、2/3は社外開発。重要なコンポーネント(例:フライトガイダンスコントロール)は、ソフトウェアを含むサブコンポーネントを自社開発。 Airbus350のサプライチェーンを別途示す。

2009年ESTEREL社ユーザコンファレンスにおけるAirBus社資料より抜粋

Airbus社製航空機のシステム(3/4)

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

- SCADEのツールをカスタマイズすることで、開発工程の競争優位性を維持する。

適用範囲・内容	モデル開発、シミュレーション、検証、自動コード生成
ツールチェーン	Airbus社の戦略 1.モデルベース開発と認定自動コード生成 2.内製のACGツールとESTERELのツールの利用 利用ツール Airbus ACG ツールセット(SCADE-KCGを含む内製ツール) SCADE、SCADE Display(ディスプレイシステムの開発) Scade Synchronous Formalism(手法) SCADE KCGでは、SCADE ACGで生成されたCコードを後処理し、モデルに影響を与えることなく、ターゲットに最適化されたコードとすることができる。 

Airbus社製航空機のシステム(4/4)

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

- SCADEを導入することで、形式手法を意識することなく安全系のシステム開発が可能となった。

開発者のスキルレベル	SCADEは、ユーザが意識することなく形式手法を利用できることを特徴としている。このため、SCADEの操作を習得した開発者がいれば開発できる。しかしながら、生成されたコードの検証やバリデーションにおいて、形式手法の概念や表記の理解が必要な場面もあり、数学的素養のあるソフトウェアエンジニアが必要となる。
開発成果	1. コーディングエラーの大幅な削減:Airbus A340 プロジェクトでは70%のコードが自動生成された。 2. 仕様変更への迅速な対応:システムモデルの仕様変更に迅速に対応を可能(仕様変更のターンアロウンドサイクルが3～4倍改善)にし、トレーサビリティも改善された。 3. 生産性の改善: 生産性が改善したことでソフトウェア規模の増大に対応することができた。 A340のプロジェクトでは、SCADEを利用することで、大幅な効率化を実現したため、SCADEをA380の開発にも採用した。 A380では、AirBus社とサプライヤがSCADEを使用した。

艦載ヘリコプタ運行限界計装システム(SHOLIS)(1/3)

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

- 英国国防省標準00-55(UK MoD 00-55)に従い開発された。

開発プロジェクトの概要	開発対象	ヘリコプタ着陸システム(Ship/Helicopter Operation Limits Instrumentation System)
	開発時期	1996年～1997年
	開発期間	2年、19人年
	開発規模	安全航行警告:Z仕様200頁、英国防衛省標準00-55(UK MoD 00-55)SIL4準拠、SPARK2.7万行
開発の背景	艦載ヘリコプタ運行限界計装システムは、ヘリコプタを艦載する船舶に搭載されるコンピュータシステムで、船舶の乗組員に、さまざまな状況での安全なヘリコプタの運行に関してのアドバイスを与える。 耐障害性のリアルタイム組込みシステムであり、初めて、安全重視ソフトウェアのための英国暫定防衛標準(IDS)00-55への適合を目指して構築された。 UK MOD 00-55では、形式安全管理と品質システム、システムのふるまいの形式仕様、形式証明(仕様レベルとコードレベルの両方)、完全に独立した検証と妥当性検証、情報フロー、タイミング、メモリ使用などのプログラム属性の静的分析を要求する。 SHOLISはのソフトウェアは、約13000の宣言と14000の記述からなる。システムユニットの位置付け、安全性インテグリティレベル、ソフトウェア危険分析などで形式手法による静的分析が行われた。安全系ソフトウェアは、仕様に対し「proof of partial correctness」により、Z表記法で記述され、属性の証明(Proof)が実行された。  	

艦載ヘリコプタ運行限界計装システム(SHOLIS)(2/3)

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

- Z表記とSPARKにより開発されSIL4を獲得した。

開発体制	– 英国防衛省(UK MOD) – PMES Ltd(Power Magnetics and Electronics Systems;現在はUltra Electronics社の一部):プライムシステムコンタラクタ – Praxis:ソフトウェア開発
適用範囲・内容	仕様記述:Z 証明(Proof) ソフトウェア記述:SPARK
ツールチェーン	SPARKツール ·エグザミナ(Examiner) – 静的セマンチックチェック – 部分コレクトネス用汎用検証条件(VCs)、予め定義されるAdaの例外を必要としない。 · シンプリファイア(Simplifier) – VC用自動 “theorem prover” · チェッカ –インタラクティブプルーフツール ·CADiZ
開発者のスキルレベル	証明は4名の技術者により行われた。2名がZの証明を担当し、その内の1名は、他のチームの2名と協力し、Z仕様に関するSPARKのアノテーションを生成し、すべてのSPSRKの証明を実施した。 データと情報フローの分析は、2名のコーディング技術者により行われた。 証明に係わった技術者は数学的素養のあるソフトウェア技術者で、ZをCSPを含む様々な形式手法プロジェクトの数年の経験がある。 SPARK Simplifier、Proof Checkerの経験のある技術者は、1名であった。 Zの証明には、Zの経験(学術的、実務的の両方)と証明の経験が必要になる。

艦載ヘリコプタ運行限界計装システム(SHOLIS)(3/3)

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

- 詳細設計、コーディングとインフォーマルテストに17%、単体テストに25%の工数がかかった。

開発成果

Integrity : SIL4
ソフトウェア規模 : 27000行(SPARK)
Defect/ksLOC : 0.22
LOC/Day : 7
Proofによる実証は、テストを実施するより、コスト面で有利であった。

工程	障害発見比率(%)	工数比率(%)
仕様作成	3.25	5
Zによる証明(Proof)	16	2.5
ハイレベル設計	1.5	2
詳細設計、コーディングとインフォーマルテスト	26.25	17
単体テスト	15.75	25
統合テスト	1.25	1
コード証明(Proof)	5.25	4.5
システム妥当性検証テスト	21.5	9.5
受入れテスト	1.25	1.5
その他	8	3.2

その他
開発チームメンバへのトレーニング : 1%
プロジェクト管理、計画 : 20%
安全管理と安全技術 : 7%
IV&Vのテストに関係しない活動 : 4%

コンポーネント仕様のモデル化(プジョー)(1/2)

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

- 車載コンポーネントの機能を形式仕様でモデル化。故障箇所を同定し、修理を可能にする。

開発プロジェクトの概要	開発対象	206、307、407モデルの部品機能仕様のモデル化(形式記述)
	開発時期	1999～2001年
	開発期間	30ヶ月
	開発規模	50Bモデル、7,000イベント、2,000の抽象変数、150,000行の書類
開発の背景	コンポーネントの詳細形式仕様がソフトウェア以外にも利用された例である。車やコンポーネントの欠陥や故障は、コンポーネントの機能が仕様に忠実でないことによる場合が多い。この診断方法では、車とコンポーネントの機能仕様を形式化(イベントBモデル化)し、Bモデルインタプリタ(BI)がコンポーネントの動作が仕様に合致しているかを確認する。この方法で車を診断する方法は以下のようになる。 －車のコンポーネントの仕様を正確に記述する(コンポーネント仕様のBモデル化) －実機能とBモデルとの厳格なリンク(ディクショナリ) －コンポーネントのふるまいとコンポーネント仕様の比較(記録分析)	
開発体制	プジョーがClearSyへ委託 1台目:14人年 2台目:5.6人年.	

コンポーネント仕様のモデル化(プジョー) (2/2)

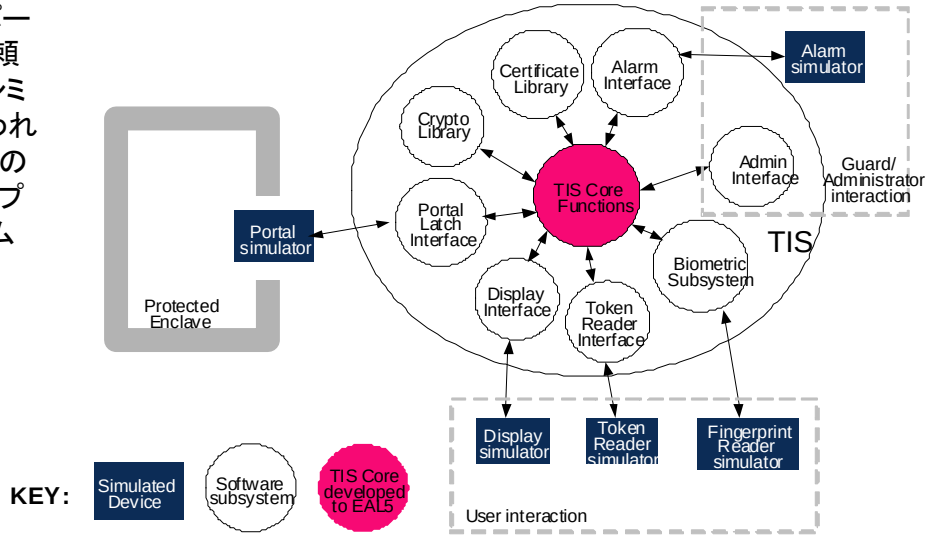
SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

適用範囲・内容	部品の機能仕様の形式化 ■Bモデル化 BI(Bモデルインタプリタ)では、自動証明を行うため、曖昧でない明確なコンポーネントの仕様記述が必要となる。そのため、車とコンポーネントのモデルをイベントBメソッドで構築した。 ■ディクショナリ コンポーネントの動作に影響を与える物理入力パラメータ(速度などの数量入力や正常、異常、重要などの質的入力)の概念を定義する。Bモデルでは、物理入力パラメータに対応する変数(B変数)が宣言される。ディクショナリは、物理入力とB変数のリンクを記述することでB変数を明確に定義する。さらにパラメータの変化とB変数の変化の整合性を維持する。 イベント(例、オイル温度が120度以上の時に起こる)を物理入力パラメータ値で定義し、定義されたイベントでの、物理入力パラメータにより起こるBモデルの期待される変化を明記する。 ■記録分析 すべてのコンポーネントをすべての場合で確認するには、非常な時間がかかるため、シナリオで故障や欠陥の影響を再現する。 BIは、シナリオに基づきイベントの発生と物理入力パラメータを継続的に観察する。主観的で、記録できないパラメータは、技術者が観察結果を記録する。 しかし、依然として、すべての観察可能なパラメータ値を記録するには、時間と資源を要するため、特定の規則を定義し推論する。 BIは、記録を分析し、異常なパラメータ値、期待されないコンポーネントの反応を検知することでコンポーネントの欠陥や故障を診断する。
ツールチェーン	Atelier B
開発成果	206、307、407モデルのモデル化 200万行の設計書に記述された52の機能についてモデル化を行った。 2車種で実施 (307、206) ー約 2 x 150,000行の書類が作成された。 ー50のBモデル、7000のイベント、2000の抽象変数で記述された。これにより98%の証明が自動的に実行された。 BI の理論は、PSAが保有している。プジョーの技術者が診断テストを定義し、PSAのホットラインの技術者が利用している。 課題 ーBモデルの開発コストの低減 ーBモデルの正確さの向上 ーBI をアプリケーションの一部として統合し実装

「Tokeneer ID Station (TIS) 」(バイオメトリクスID認証ツールのアクセス管理セキュリティソフトウェア)(NSA)(1/4)

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

- 米国NSAから委託を受けPraxisが開発。

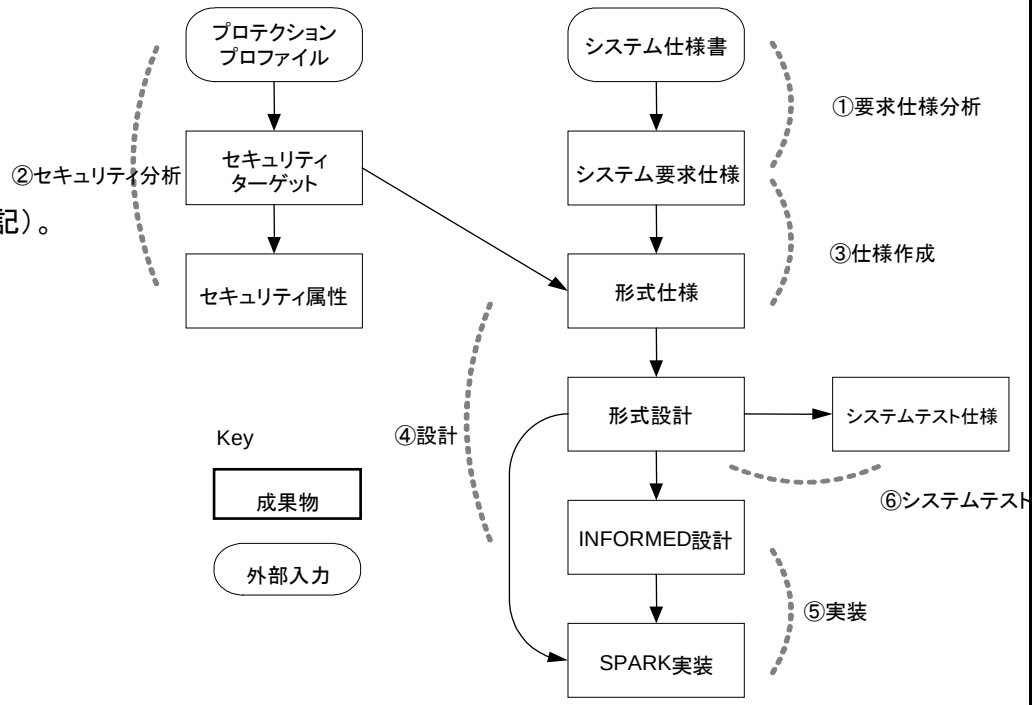
開発プロジェクトの概要	開発対象	「Tokeneer ID Station (TIS) 」(バイオメトリクスID認証ツールのアクセス管理セキュリティソフトウェア)
	開発時期	2003年
	開発期間	9ヶ月/260人日
	開発規模	TISコア　9,939(Ada)、16,564行(SPARKアノテーションとコメント) サポートソフトウェア　3,697行(Ada)、2,240行(SPARK/アノテーションとコメント) 機能仕様　100ページ(Z表記) 費用:250,000ドル
開発の背景	「Tokeneer」システム(TIS)は、元々NSAで開発されたEAL5に準拠するシステムの開発を可能とするセキュリティソフトウェアである。NSAでは、様々なバイオメトリクス認証のアクセス管理の研究がされている。 Praxis HISは、複数のアプリケーションが単一のスマートカードに存在することを可能とするマルチアプリケーションオペレーティングシステムの開発、MULTOSプロジェクトを2002年に完了した。MULTOSプロジェクトの成功が、NSAによるTISプロジェクト(セキュアなソフトウェアエンジニアリングの実証実験プロジェクト)提案の契機となった。 PRAXISは、9ヶ月に渡る開発を2003年に固定費用(費用は未公開)でTISプロジェクトをNSAから受託した。 TISプロジェクトでは、トーケナーシステムのコンポーネントの1つが再開発された。この際に独立系信頼性コンサルタント(SPRE社)により、TISデバイスシミュレータが開発され、TISの実機の代替として使われた。TISプロジェクトの資料は、NSA技術移転契約の下に2008年10月に公開され、英国のアカデミックプロジェクトであるGC(グランドチャレンジ)プログラムのプロジェクトである「Verified Software Grand Challenge」で活用された。  システムの概観

「Tokeneer ID Station (TIS) 」(バイオメトリクスID認証ツールのアクセス管理セキュリティソフトウェア)(NSA) (2/4)

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

- ZとSPARKにより3名の技術者が9ヶ月で開発

開発体制	NSA (National Security Agency),の下、Praxis HISが開発、一部の工程をSPREE社が実行 Prxis HIS SPRE プロジェクトは、3名のスタッフ体制で260人日、9ヶ月を要した。
適用範囲・内容	1. 要求仕様分析 Praxisが開発したRevealと呼ばれる手法で要求仕様を分析する。 2. セキュリティ分析 プロテクションプロファイルから、セキュリティターゲットとセキュリティポリシモデルを開発する。 3. 仕様作成 要求仕様を正確に形式的に記述する(Z表記)。 4. 設計 形式仕様を詳細化する(Z表記)。 実装モジュール(SPARKパッケージ)を開発するためのガイド(INFORMED設計)を作成する。 5. 実装 INFORMED設計に従い形式仕様をSPARK(Adaのサブセット)で実装する。 6. システムテスト SPARKと静的チェックツールを使い、実装コードをテストする。



「Tokeneer ID Station (TIS) 」(バイオメトリクスID認証ツールのアクセス管理セキュリティソフトウェア)(NSA) (3/4)

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

- EAL5を超えるセキュリティレベルを達成した

ツールチェーン	REVEAL(要求仕様管理のメソッド;ツールではない) fuzz type checker (Zのチェック) SPARK Adaコア システムのコアとなる機能は、AdaのサブセットであるSPARKとツールセットにより開発された。 コア機能と周辺を接続するサポートソフトウェアはAdaで開発された。
開発者のスキルレベル	開発者のスキルをA,B,Cに分けると、A レベルの開発者2名、Bレベルの開発者1名が開発に当たった。Aレベルの開発者は、Zの記述と解読ができるスキルがあることに加え、セキュリティなどの専門的技術を有する。Bレベルの開発者は、Zの解読はできるが、記述をするスキルは不十分であった。
開発成果	個別の信頼性テストと2003年の納入以来、発見された欠陥は4個であった。 その1つは、プロジェクト完了後のコードテストで発見された。2つめのバグは、証明(Proof)を実施中に発見された。 ファイルから読込まれた整数を検証するコードのバグで、「秒(Seconds)」を表わす整数が、1/10秒に変換される際にオーバーフローエラーを起こした。 SPARKツールは、部分的コレクトネスとランタイムエラーの検証条件を生成するが、Adaのオーバーフローチェックの検証条件が生成されなかった。その後のツールの改善で検証条件が再生成されバグが発見された。その他にSPRE社のプロジェクトチームがテストで障害を発見した。 両社とも、TISのコアの間違いよりも、ユーザマニュアルの不備を心配している。 納入以来、システム分析のための利用や試行では欠陥は発見されなかった。 工数比率のシステムテストには、SPRE社のテストへの貢献は入っていない。おそらく25%ほどと推測される。 機能仕様は、100ページほどのZ表記と英文の説明から構成される。NSAからの依頼は、EAL5に準拠するシステムの開発であった。Praxisは、多くの領域でEAL5の要求以上の条件を達成した。厳格な技術を使用したことが結果的に効率的であったと言う。

「Tokeneer ID Station (TIS) 」(バイオメトリクスID認証ツールのアクセス管理セキュリティソフトウェア)(NSA) (4/4)

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

開発成果

	プログラムサイズ(LOC)		生産性(LOC/日)	
	ADA	SPARK アノテーションとコメント	コーディング時	全体
TIS コア	9939	16564	203	38
サポートSW	3697	2240	182	88

工程	工程比率(%)	工数(人日)
プロジェクト管理	11	28.6
要求仕様	10	26
システム仕様	12	31.2
TISコア機能設計	15	39
TISコア実装と証明(Proof)	29	75.4
システムテスト	4	10.4
サポートソフトウェアとの統合	16	41.6
受入れテスト	3	7.8
合計	100	260

IPA Software Engineering Center
Information-technology Promotion Agency, Japan

形式手法ツールベンダ調査

ClearSy

Esterel Technologies

Praxis HIS(High Integrity Systems)

Verum

Escher Technologies

ClearSy(1/2)

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

- 企業情報
  - 企業名
    - ClearSy
  - 所在地
    - 13857 AIX EN PROVENCE CEDEX 3（仏）
  - 概要
    - フランスのシステム開発企業として、鉄道や原子力などの安全系システムソフトウェアを受託開発する。またツールベンダとして、Bメソッドによる形式手法ツールであるAtelier Bを開発、提供する。
      - 2001年1月設立（Steria社；仏総合ITベンダからのスピンアウト）
      - Steria 65%、Teamlog（仏NWベンダ）35%出資
      - 社員数40名、うち形式手法エンジニア30名
      - 07年売上高：2.7百万ユーロ（約3.2億円、1ユーロ120円換算）
    - 主要顧客
      - 政府官公庁・研究機関： CEA（仏原子力庁）、CNES（国立宇宙研究センター）、SNCF（仏国鉄）、RATP（パリ運輸局）等
      - 航空機： EADS（欧州航空防衛大手）、Eurocopter等
      - 自動車： Peugeot、Renault、BOSH
      - 重工・運輸： Althom、Atmel、THALES、Siemens Transportation Systems （STS）
      - エレクトロニクス・IT： STMicroelectronics、Nokia、Gemplus（スマートカード）、SVE（Dassault）
      - 金融： Société Générale

ClearSy(2/2)

■ 製品情報

- Atelier B
  - Atelier BはBメソッドを利用した形式手法に基づく、システム、ソフトウェアの仕様記述、モデリング、検証のツールである。B表記で記述された仕様を、段階的な詳細化技法によって仕様から実装可能な詳細レベルにまで詳細化をする。
  - B表記で記述された仕様（モデル）は、段階ごとに証明され、重大な障害がないことを確認しながら詳細化が進められる。
  - 詳細化された、詳細仕様（モデル）は自動コード生成によりAdaやCなどの実行言語に変換される。
  - 主な機能
    - Bファイルの静的チェック（文法、タイプチェック、ビジビリティチェック等）
    - 証明責務の生成
    - 自動とインタラクティブな詳細化
    - 自動とインタラクティブな証明
    - Bインプリメンテーションの従来言語（Ada等）への変換

- Atelier BとBメソッドの経緯
  - Jean-Raymond AbrialがOxford大学でZ-表記に引き続き概念を開発（1985）
  - BP出資の研究プロジェクト（BP IT 部門とOxford）で体系整理(1985-1988)
  - Digilog社-GEC Alstom社がAbrielの協力によりAtelier Bツールキット開発（1988-1992）
  - RATP、INRET、SNCFのプロジェクトでAtelier B強化

Esterel Technologies（1/2）

SEC
Software Engineering
for Mo･No･Zu･Ku･Ri

■ 企業情報

- 企業名
  - Esterel Technologies
- 所在地
  - Parc Euclide8 rue Blaise Pascal 78996 Elancourt （仏）
- 概要
  - フランスの形式手法ツールベンダとして形式手法ツールSCADEを開発し販売している。SCADEは、航空機、原子力や鉄道などの安全系システムソフトウェアの開発に使われている。
    - 社員数100名強
    - 08年売上高：15百万ユーロ（約18億円、1ユーロ120円換算）
    - 開発支援ツールSCADE SuiteやSCADE Displayを販売
    - DO178-B Level A、IEC61508 SIL3、IEC60880準拠
  - 系譜
    - （1986年）Verilog社（ソフトウェア・ベンチャー）がMerlin Gerin（現Schneider Electric傘下・ブランド名）の内製ツールSagaとAérospatiale社（現AirBus社）のツールSAOを統合し商用化
    - （1999年）Telelogic社がVerilog社においてSCADEを開発途中にVerilog/SCADEを買収
    - （2001年）Esterel社がSCADE部門をTelelogicより買収（2001年11月）

Esterel Technologies（2/2）

SEC
Software Engineering
for Mo･No･Zu･Ku･Ri

- 主要顧客
  - 航空機・防衛（全売上の55%）

    Airbus（同社7割の組込み系システムがSCADEを活用）、Dassault Aviation、DS&S（Rolls-Royce)、ELTA（Areva）、EADS（欧州航空防衛大手）、Eurocopter、General Dynamics、Honeywell、Lockheed Martin、NASA、Pratt & Whitney、Rockwell Collins、Safran、Sagem（Airbus下請け）、Thales DAE、US Air Forces、など
  - 鉄道（同25%）：

    Althom、Ansaldo Signal、BJTU（中国）、SNCF（仏国鉄）、RATP（パリ運輸局）、Thales Rail Signaling Systems、Siemens Rail Transportation、など
  - 自動車・発電他（同20%）：

    GM、ホンダ、日産、Peugeot、Renault、スバル、トヨタ、Volvoなど、韓国電力、三菱、BARC（Bhabha Atomic Research Center、印）、DS&S、KAERI（Korea Atomic Energy Research Inst.）など

■ 製品情報

- SCADE Suite
  - ソフトウェア要件管理
  - ソフトウェア開発（制御モデル設 計）
  - 検証(シミュレーション、形式検 証)
  - 自動コード生成 Cコードとの一致性を保証
  - IEC-61508 SIL3/SIL4認証を取得制御モデルと自動生成される
- SCADE表記
  - 1900年代に、リアルタイム制御ソフトウェアを記述するコンピュータ言語として、INPGにより、Lustre表記(Lustre V3) 定義された。
  - 現ESTREL社のChief Scientistである G. BerryらがEsterel意味論定義（1984年）
  - EsterelとLustreが統合され現在のSCADE表記となる。

Praxis HIS（High Integrity Systems）（1/2）

SEC
Software Engineering
for Mo･No･Zu･Ku･Ri

■ 開発企業
- 企業名
  - Praxis HIS（High Integrity Systems）
- 所在地
  - Bath（英）
- 概要
  - 高信頼性・安全性システム、ソフトウェア・インテンシブなシステムに特化したシステム・エンジニアリング会社。航空機・国防領域を中心とした実績を持ち、EU FP6/RODINに参画。社員数100名強
  - 旧名Praxis Critical Systems、04年、HIS Consultingと合併、現社名へ、仏エンジニアリング会社Altranグループ
  - 売上規模： 11.5百万ﾎﾟﾝﾄﾞ（約16億円、1ポンド140円換算）
  - エンジニア100名強
  - 航空機領域からスタート、現在、セキュリティ関係にも強み
  - Adaのサブセット言語ツールSPARKを適用・販売
- 系譜
  - 1983年： Praxis PLC設立、SWへエンジニアリング原則を適用
  - 1985年： HIS、国防領域に強み発揮
  - 1990年： Praxis PLC、Deloitte Consultingにより買収
  - 1993年： Praxis、SPARK開発のProgram Validation社（PVL）買収
  - 1995年： HIS、仏Altran傘下へ
  - 1997年： HIS、宇宙・運輸・製薬・金融領域へ事業拡大
  - 1999年： Praxis、Altranにより買収
  - 2001年： Praxis、英Bathに本社拠点設立
  - 2004年： PraxisとHISが合併、Praxis HIS設立
  - 2008年： 9月、Altran社内にパリ事務所開設

Praxis HIS（High Integrity Systems） （2/2）

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

- 主要顧客
  - 航空機： BAE Systems、EuroFigher Consortium、Lockheed Martin、NATO、Rockwell Collins、Rolls-Royce
  - 重工・運輸： Althom、General Dynamics UK、Thales UK
  - IT・技術： AdaCore（ツールベンダー、戦略提携、08年10月）、
  - QinetiQ（ナノテクノロジー）、米NSA（National Security Agency）

■ 製品

- SPARK toolset/SPARK Pro
  - Ada 83を元にSouthampton大学で英国防衛省の支援を受け開発された（1983年）。その後Program Validation社、さらにはPraxis HIS社により拡張、改善された。
  - AdaのサブセットとしてSPARKは、煩わしい言語機能を取り除き、機能を制限する。その代りにアノテーションにより付加情報を提供できる。Zで記述された機能仕様がSPARKにより詳細化される事例が多くある（Praxisの事例）
  - 主な機能
    - 静的チェック、情報フロー分析、 検証条件(VC)設定（Examiner）
    - 自動数理証明（検証条件に基づく検証）（Simplifier）
    - 証明チェック（自動数理証明で取残された証明の実行） （Proof Checker）

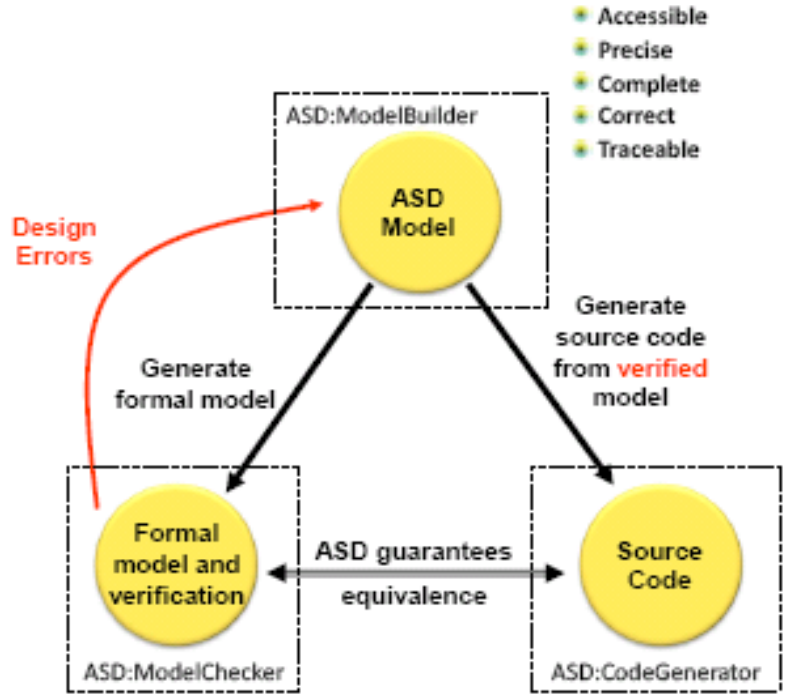
Verum(1/2)

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

■ 企業情報
- 企業名
  - Verum Consultants BV
- 所在地
  - Laan van Diepenvoorde 32　5582 LA Waalre（オランダ）
- 概要
  - オランダのEindhoven近郊にある形式手法に基づく分析ツールをSaaS方式で提供する2004年設立のスタートアップ企業
    - 社員数　50名（推定）
    - 売上げ高：814,000ユーロ（予定）
  - 系譜
    - Philippa Hopcroft女氏は、FDR（CSPによる並行プロセスのモデル検証ツール）を開発したOxford大学コンピュータサイエンス学部Bill Roscoe教授（T Hoareに師事）の研究室で学んだ。
    - その後、同女氏は、父親であるGuy BroadfootとVerum社を設立し、 ASD（ Analytical Software Design；分析ソフトウェア設計）を開発した。
    - ASDは、CSPによるモデル検証ツールであるFDR（Oxford大学で開発され、Formal Systems社により開発、販売されている）や自動コード生成機能などを組合せた形式手法ツールである。
  - 主要顧客
    - Philips Applied Technologies、 Philips Healthcare 、NXP、NandaTech、FEI、ASMI、CCM、Sioux、TASS、その他
- 製品
  - ASD：モデルビルダ
    - ASDモデルビルダは、Windowsアプリケーションとして、ユーザのデスクトップコンピュータにインストールされる。ユーザは、表形式の入力方式を採用することで、形式手法に基づく数式入力に比べ、簡単にモデル入力をすることができる。
  - ASD：モデルチェッカ
    - ASD：モデルチェッカは、ホスティングサービス（SaaS）として提供され、ASD設計モデルの数式検証を実行する。ここで発見された不具合は、ASD：モデルビルダで修正される。ASD：モデルチェッカは、 Formal Systems社のFDRをコアとして採用している。

Verum(2/2)

- ASD：コード生成
  - ASD：コード生成は、ホスティングサービスで提供される。ASDモデルをC++やC#などの言語に変換する。
  - 現在、C++とC#への変換ツールがある。
- ASDポータル
  - ASDポータルWebサイトは、ASDサービスを提供、管理するサイトである。



Escher Technologies (1/2)

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

■ 企業情報
- 企業名
  - Escher Technologies
- 所在地
  - Mallard House, Hillside Road, Ash Vale, Aldershot GU12 5BJ（英）
- 概要
  - 1995年にDavid Crocker氏により設立された従業員数、数名の企業。
  - David Crocker氏の略歴
    - 1977年にCambridgeのDowning Collegeにおいて、自然科学の修士を取得、その後博士号を取得した。複数の独立コンピュータ企業で働いた後、OS、ネットワーク、通信を専門とするソフトウェアコンサルティング企業を設立した。
    - 同氏は、 人工知能と「provably-correctソフトウェア」（証明可能な正しいソフトウェア）に長年にわたり関心を持っていた。その後、1995年に、その考えを実現するためにEscher Technologies社を設立し、2000年にPerfect Developerの初版をリリースした。
  - 同社は、York大学のJim Woodcock氏がチェアマンを努めるGrand ChallengeのVerified Software RepositoryのMondex smart cardのプロジェクトに参加している。
  - Grand ChallengeのVerified Software Repositoryは、形式手法で開発されたMondex smart cardを複数の手法で再検証するプロジェクトであり、下記の研究者が参加している。
    - Daniel Jackson (MIT) Alloy
    - Michael Butler (Southampton) B .
    - Cliff Jones (Newcastle) VDM
    - Martin Gogolla (Bremen) OCL.
    - Jim Woodcock (York) Z
    - Chris George (Macau) Raise.
    - David Crocker (Escher) Perfect Developer
- 主要顧客
  - General Dynamics UK Ltd.

Escher Technologies (2/2)

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

- 製品
  - Perfect Developer (PD)
    - 独自表記、Perfect Language を採用した形式手法に基づくツール。主に、ITシステムや、航空関係のシステムを開発に使われている。
    - その理念は、形式仕様を開発し、実装可能な仕様まで詳細化をすることにある。形式手法のツールではあるが、高度な数学的な知識を必要としない。
    - Perfect specification表記は、オブジェクト指向のスタイルで記述され、JavaやC#、C++のコードの生成を可能とする。
    - Perfect Developerはシステムをモデル化するためのツールであり、「正しさの形式証明」（formal proofs of correctness）とモデルからコードを自動生成する機能を提供する。

Software
Engineering
Center
Information-technology Promotion Agency, Japan

形式手法の技術者向け教育研修調査

ClearSy

Esterel

Praxis HIS

Adelard

B-Core

Verum

QAI EdistaLearning

形式手法の教育／トレーニング

SEC
Software Engineering
for Mo・No・Zu・Ku・Ri

- 教育・研修機関について
  - 形式手法に関する教育やトレーニングは、ツールベンダを中心に、ユーザへのツールのオペレーショントレーニングの一環で行われている場合が多い。
  - 独立した教育機関やトレーニングサービス企業が形式手法の教育やトレーニングを行っている例は少ない。下記にトレーニングサービスを行う企業を示す。

名称	国	所在地	設立	事業内容
ClearSy	フランス	Guillibert Gauthier de la Lauziere Aix-en-Provence les Milles	2001年	ツール、開発サービス、トレーニング
Esterel	フランス	Parc Euclide 8 rue Blaise Pascal 78996 Elancourt	1984年	ツール、トレーニング
Praxis High Integrity Systems Limited	イギリス	20 Manvers Street Bath BA1 1PX	1982年	研究開発、研修
Adelard	イギリス	College Building 10 Northampton Square London	1987年	コンサルティング、セーフティぇースリサーチ、ツール、研修等
B-Core	イギリス	Kings Piece Harwell Oxon OX11 0PA	1993年	Bツールキット開発、販売研修
Verum	オランダ	Eindhoven	2004年	ASD
QAI EdistaLearning	USA	2101 Park Center Dr., Suite 200 Orlando, FL 32835-7614	1980年	トレーニングサービス

形式手法の教育／トレーニング：ClearSy（仏）

SEC
Software Engineering
for Mo・No・Zu・Ku・Ri

- ClearSy
  - 組織プロファイル
    - フランスのシステム開発企業として、鉄道や原子力などの安全系システムソフトウェアを開発を受託開発する。またツールベンダとして、Bメソッドによる形式手法ツールであるAtelier Bを開発、提供する。
  - 教育・研修体系における形式手法の位置づけ
    - 提供するツールの操作トレーニングの一環で形式手法の教育をする。
  - カリキュラム
    - Method B Training Level 1 : Understanding B
      - Bメソッドの規範の基礎の理解
      - 4日間、2,130ユーロ
    - Method B Training Level 2 : Practicing B
      - Bプロジェクト開発規範の理解
      - 「good」Bモデル構築の練習
      - B言語のコンセプト：上級.
      - イベントドリブンBについて
      - 4日間、2,130ユーロ
    - Method B Training Level 3: Prove B
      - Bモデルの証明を学習するワークショップ
      - 3日間、1,780ユーロ
    - BART Tool Training Level 4：自動詳細化
      - BARTツールによるBモデルの自動リファイン（詳細化）を学習する。
      - 3日間、1,780ユーロ
  - 企業における活用状況
    - STSなどのユーザ企業がツールベンダが提供する教育／トレーニングを利用する。

形式手法の教育／トレーニング：Esterel(仏)

SEC
Software Engineering
for Mo・No・Zu・Ku・Ri

- Esterel
  - 組織プロファイル
    - フランスの形式手法ツールベンダとして形式手法ツールSCADEを開発し販売している。SCADEは、航空機、原子力や鉄道などの安全系システムソフトウェアの開発に使われている。
  - 教育・研修体系における形式手法の位置づけ
    - 提供するツールの操作トレーニングの一環で形式手法の教育をする。
  - カリキュラム
    - Course 1: Two Day Overview
      - SPARKを利用した高信頼性ソフトウェア開発技術の規範と実践に関する管理者と技術者向けチュートリアル
    - Course 2: Software Engineering with SPARK
      - 高信頼性ソフトウェア開発の規範と認証の要求について示し、SPARK Examinerの説明と実習を管理者、規制担当者、技術者向けに行う。
    - Course 3: Advanced SPARK Program Design and Verification
      - SPARKを利用した証明や検証について習得する上級コース
    - Course 4: Concurrent Software Design with RavenSPARK
      - Ada95のサブセットを定義するRavenscarプロファイルについて説明する。
    - Course 5: Introduction to the Proof Checker
      - SPARK 証明チェッカについて説明する。
    - Course 6: UML to SPARK
      - UMLからSPARKを生成する理論について説明する。
  - 企業における活用状況
    - AirBusなどのユーザ企業がツールベンダにより提供される教育／トレーニングを利用する

形式手法の教育／トレーニング：Praxis HIS(英)

SEC
Software Engineering
for Mo・No・Zu・Ku・Ri

- Praxis HIS
  - 組織プロファイル
    - 高信頼性・安全性システム、ソフトウェア・インテンシブなシステムに特化したシステム・エンジニアリング会社。航空機・国防領域を中心とした実績を持ち、EU FP6/RODINに参画。教育・研修体系における形式手法の位置づけ
    - 提供するツールの操作トレーニングの一環で形式手法の教育をする。
  - カリキュラム
    - Course 1: Two Day Overview
      - SPARKを利用した高信頼性ソフトウェア開発技術の規範と実践に関する管理者と技術者向けチュートリアル
    - Course 2: Software Engineering with SPARK
      - 高信頼性ソフトウェア開発の規範と認証の要求について示し、SPARK Examinerの説明と実習を管理者、規制担当者、技術者向けに行う。
    - Course 3: Advanced SPARK Program Design and Verification
      - SPARKを利用した証明や検証について習得する上級コース
    - Course 4: Concurrent Software Design with RavenSPARK
      - Ada95のサブセットを定義するRavenscarプロファイルについて説明する。
    - Course 5: Introduction to the Proof Checker
      - SPARK 証明チェッカについて説明する。
    - Course 6: UML to SPARK
      - UMLからSPARKを生成する理論について説明する。
  - 企業における活用状況
    - ユーザ企業がツールベンダにより提供される教育／トレーニングを利用する。

形式手法の教育／トレーニング：Adelard（英）

- Adelard
  - 組織プロファイル
    - Adelardは1987年に設立された独立の専門コンサルティング企業である。ロンドン市立大学の構内にオフィスを設置し、同大学の教授を勤める研究者数名が、Adelard社の上級社員となっている（社員数は14名程度）。EUのFPプロジェクトに参加が同社の研究開発の重要な一部分となっている。Adelard社は安全系システムの開発コンサルティングを主な業務としており、その中には、防衛システムなどの公共関連プロジェクトが多くある。
    - 同社が開発したセーフティケースツールを利用したセーフティケース作成プロジェクトやVDMなどの形式手法を採用したプロジェクトなどの安全関連プロジェクトを実施している
    - 所在地：College Building 10 Northampton Square London EC1V 0HB（英）
  - 教育・研修体系における形式手法の位置づけ
    - 下記のカリキュラムは、大学の学生向けのカリキュラム（20時間／1学期）であるが必要に応じ、同社顧客向けにも実施する。
  - カリキュラム
    - 数学的背景
      - プログラム言語意味論
      - 集合論、タイプ理論
    - 仕様言語
      - Z
      - B / Rodin
    - 統語解析アプローチ
      - コーディングスタイルチェック–e.g., MISRA-C
      - ツール：Safer C、Coverity、QAC
    - 意味解析アプローチ
      - Hoare-logic証明
      - モデル検証
      - ツール：Frama-C、VCC、CBMC、Java Pathfinder、Spin、SPARK Ada

形式手法の教育／トレーニング：B-Core（英）

SEC
Software Engineering
for Mo・No・Zu・Ku・Ri

- B-Core
  - 組織プロファイル
    - Bのツールを提供している。同社のキーパーソンの健康上の理由により、現在は積極的な活動をしていない。
    - 所在地：Kings Piece Harwell Oxon OX11 0PA（英）
  - 教育・研修体系における形式手法の位置づけ
    - 提供するツールとBに特化した形式手法の教育をする。
  - カリキュラム

    先進技術の移行を成功させるには、高品質な、焦点が良く合うトレーニングが、顧客の要求に沿った形で必要になる。

    B-Coreはオンサイトあるいは、B-Coreのオフィスで、トレーニングパッケージを提供する。
      - ソフトウェア開発の厳格な開発手法について
      - システム技術での集合論の利用
      - B言語を利用してシステムを定義する方法
      - オブジェクト指向システムの構築
      - 詳細化による設計
      - 階層化システム開発
      - ソフトウェアシステムの正当性（Correctness）

形式手法の教育／トレーニング：Verum（オランダ）

SEC
Software Engineering
for Mo・No・Zu・Ku・Ri

- Verum
  - 組織プロファイル
    - オランダのEindhoven近郊にある形式手法に基づく分析ツールをSaaS方式で提供する2004年設立のスタートアップ企業
  - 教育・研修体系における形式手法の位置づけ
    - 提供するツールの操作トレーニングの一環で形式手法の教育をする。
  - カリキュラム
    - Starting ASD
      - 3日間コース：1,800ユーロ
      - ASDの基礎を学習する3日間のコース。ASDインタフェースと設計モデルの構築と検証の方法、自動コード生成など、ASDスィートの使い方を学習する。
      - このコースは、ASDの利用を始めるソフトウェアアーキテクト、ソフトウェア設計者を対象とする。ASDスィートについての事前知識は必要としない。
    - Mastering ASD
      - 2日間コース：1,200ユーロ
      - 前コースの拡張コース。複数のアーキテクチャ／設計パターンと効果的なASDの利用方法を学習する。
      - また、いくつかの先進的モデルチェックとコード生成の機能についても学習する。
      - このコースは、ASDを個々のソフトウェアコンポーネントではなく、システムに適用するソフトウェアアーキテクトと設計者を対象とする。
  - 企業における活用状況
    - ユーザ企業がツールベンダにより提供される教育／トレーニングを利用する。

形式手法の教育／トレーニング：QAI EdistaLearning(米)

SEC
Software Engineering
for Mo・No・Zu・Ku・Ri

- QAI EdistaLearning
  - 組織プロファイル
    - QAI Global Instituteは、1980年に米国で設立された。それ以来、プロセス管理における品質、生産性、効果的ソリューションを改善することを目指すeラーニングコースを提供する。このeラーニングのプラットフォームであるEdistaLearningにより、組織の競争優位性の開発、プロセスの拡張、組織の業績を改善するための知識の管理を支援する。
    - 所在地：Orlando, FL(米)
  - 教育・研修体系における形式手法の位置づけ
    - EdistaLearningでは、ソフトウェア技術と品質管理に関する45のオンラインコースを設けている。その中の、先進ソフトウェアプロセスモデルに形式手法が含まれる。
  - カリキュラム

    コース名：先進ソフトウェアプロセスモデル
    - 概要

      プロセスモデルは、技術開発とそれを支援するツールに適合する環境を提供する。ソフトウェアプロセスモデルは、単純な従来型のモデルから先進的なソフトウェアプロセスモデルまで多岐に渡り、安全とミッションクリチカルなシステムに適用される。

      インターネットを基盤とする今日の環境では、ソフトウェア開発の期間が数週間

      インターネットを基盤とする今日の環境で、ソフトウェアプロジェクトがほんの数週間の期間で収まることも多い。このようなプロジェクトにはビジネスクリチカルな小規模の製品の開発があり、顧客の要求に適応し、さらにプロジェクトの期限に合致することが重要となっている。コンポーネントベースプロセスモデル、クリーンルームソフトウェア技術、アジャイルプロセスモデルなどの先進的ソフトウェアプロセスがこの要求に応える。
    - 先進的ソフトウェアモデルコース
      - コンポーネントベースプロセスモデル
      - 形式手法
      - クリーンルームソフトウェア技術
      - アジャイルプロセスモデル
    - 時間

      7.5時間
    - 価格

      65ドル

IPA Software Engineering Center
Information-technology Promotion Agency, Japan

国際標準・調達規定等における形式手法適用状況調査

主要なソフトウェア開発標準の対応状況

ISO/IEC61508(機能安全)

EN 50128、IEC62278、IEC62279(鉄道)

ISO/IEC 15408(セキュリティ)

FIPS 140-2(暗号技術)

政府・公共調達等における形式手法適用状況

形式手法の利用を推奨する国際標準：主要なソフトウェア開発標準の対応状況

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

- ソフトウェア開発に関連する国際標準の形式手法への対応を示す。

国際標準	対象	形式手法についての記述
ISO/IEC 61508	機能安全（一般）	SIL2、SIL3で推奨、SIL4で強く推奨（別頁参照）
CENELEC EN 50128	機能安全（鉄道）	SIL1、SIL2で推奨、SIL3、SIL4で強く推奨（別頁参照）
ISO/IEC 26262	機能安全（自動車）	ISO/WD26262（注）のASIL Cにおいて形式手法と仕様作成でのコンピュータツールの使用が要求される予定
RTCA DO-178C	航空	DO-178Bでは形式手法に触れている程度だが、DO-178CではSWの設計と仕様での形式手法の利用が明確な記述となる予定
UK Def. Stan. 00-55	防衛	形式手法を有効なメソッドとする記述がある。
ESA 91　PSS-05-0	宇宙	ZやVDMの使用を検討すべきと記述
ISO/IEC 15408	セキュリティ	EAL7でサブシステムレベルまで形式表現されることを評価基準とする（別頁参照）
IEC 60880	原子力	記述なし
EN 62304	医療機器	記述なし
EN 50271·EN 50402	ガス測定、検出装置	記述なし
FIPS 140-2	米国政府の 連邦情報処理標準	レベル4で形式手法について言及

注：2010年制定予定のワーキングドラフト

形式手法の利用を推奨する国際標準：ISO/IEC61508（機能安全）

SEC
Software Engineering
for Mo・No・Zu・Ku・Ri

- 機能安全の国際標準である ISO/IEC61508では、SIL2以上で形式手法の使用を推奨している。

推奨技術（ISO/IEC61508）

技術、対策	参照先	SIL1	SIL2	SIL3	SIL4
1.コンピュータ支援仕様作成ツール	B.2.4	R	R	HR	HR
2a. 準形式手法	Table B.7	R	R	HR	HR
2b.. 形式手法、例としてCCS、CSP、HOL、LOTOS、OBJ、temporal logic、VDM、Zがある。	C.2.4	–	R	R	HR
ノート1－ソフトウェア安全要求仕様は、常に自然言語での問題の記述とアプリケーションを反映する何らかの必要な数学的表記を必要とする。 ノート2－表は、ソフトウェア安全仕様を明確かつ正確に定義する追加の要求事項を示す。					
＊適切な技術／対策が安全の完全性の程度に応じて選択される。代替となる、あるいは同等の技術／対策が添付の数字で示される。選択される代替となるある いは同等の技術／対策は1つに限られる。					

NR　記述された技術や対策は、所定のSILには推奨されない。実際にそのSILでの使用はしないほうが良い。

–　その技術／対策の使用を推奨もしないし、反対もしない。

R　その技術／対策の使用を推奨する。

HR　その技術／対策の使用を強く推奨する。しかるに、その技術／対策を使用しない場合は、使用しない合理的な説明と説明書が提出され、安全計画のプロセスで適合するアセッサに容認される必要がある。

準形式手法：数理的な証明に拠らない形式的な設計や仕様の記述方法、有限要素機械、状態遷移図、タイムペトリネットなど

プロジェクトの例

対象	開発企業	形式手法
SIL4プロジェクト		
防潮可動堤開閉意志決定システム	CMG Den Haag（オランダ）	Z, Promela
パリ空港シャトル自動運転システム	STS（仏）	B
SIL3プロジェクト		
パリ地下鉄プラットフォームドア	ClearSy	B
SafeRTOS	Wittenstein HIS（英）	未使用
Ccode generator, SCADE Suite KCG	ESTEREL（仏）	–

形式手法の利用を推奨する国際標準：EN 50128、IEC62278、IEC62279（鉄道）

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

- 鉄道に関する欧州国際標準であるEN 50128では、SIL1以上で形式手法（Bメソッドを例に含む）の使用が推奨されている。
- またISO/IECの鉄道に関する標準として、ISO/IEC61508を元にした国際標準、IEC62278、IEC62279（注）がある。

推奨技術（EN50128）

技術、対策	参照先	SIL0	SIL1	SIL2	SIL3	SIL4
1.. 形式手法、例としてCCS、CSP、HOL、LOTOS、OBJ、temporal logic、VDM、Z、Bがある。	B.30	-	R	R	HR	HR
2. 準形式手法	D.7	R	R	R	HR	HR
3. 構造化手法、例としてJSD、MASCOT、SADT、SDL、SSADM、Yourdonがある	B.60	R	HR	HR	HR	HR

1. ソフトウェア安全要求仕様は、常に自然言語での問題の記述とアプリケーションを反映する何らかの必要な数学的表記を必要とする。
2. 表は、ソフトウェア安全仕様を明確かつ正確に定義する追加の要求事項を示す。このれの中で1つあるいはそれ以上の技術が選択され、利用されるソフトウェアの安全度水準を満たさなければならない。

F	禁止
R	推奨
HR	強く推奨
M	義務

プロジェクトの例

対象	開発企業	形式手法
SIL4プロジェクト		
サンパウロ 地下鉄4号線 CBTC	STS（仏）	B
サンパウロ 地下鉄2号線CBTC	ALSTOM（仏）	B
パリ空港シャトル 自動運転システム	STS（仏）	B
北京地下鉄 ATCシステム	ALSTOM（仏）	B
SIL3プロジェクト		
パリ地下鉄プラットフォームドア	ClearSy	B
サンパウロ地下鉄 2号線と3号線PFドア	AES（ブラジル）	B
サンパウロ地下鉄 2,3,4号線PFドア	POSCON（韓国）	SCADE

準形式手法：数理的な証明に拠らない形式的な設計や仕様の記述方法、有限要素機械、状態遷移図、タイムペトリネットなど

注）IEC62278：鉄道システムの信頼性、可用性、保守性、安全性に関する規格）、IEC 62279：鉄道の制御、保護ソフトウェアに関する規格

形式手法の利用を推奨する国際標準:ISO/IEC 15408(セキュリティ)

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

- 国際標準ISO/IEC15408では、EAL7で形式手法の使用が必須となっている。情報技術セキュリティの観点から情報技術製品、システムが適切に設計、実装されていることを評価するための規格でコモンクライテリア(CC)と呼ばれる。

推奨技術

EAL	名称	評価概要
EAL7	Formally verified designed and tested	サブシステムレベルまでの設計が形式的表現、開発者による分析・テストの全てを評価者が再確認
EAL6	Semiformally verified designed and tested	モジュールレベルまでの設計が準形式的表現、非常に高度の攻撃に対抗
EAL5	Semiformally designed and tested	実装表現レベルのセキュリティ機能を全て確認、サブシステムレベルまでの設計が準形式的表現、隠れチャネル分析、高度の攻撃に対抗
EAL4	Methodically designed, tested, and reviewed	モジュールレベルまで確認、実装表現レベル(最も具体的レベルの設計:例えばソースコードレベル)の部分的確認、普通程度の攻撃に対抗
EAL3	Methodically tested and check	サブシステムレベルまでの開発者テスト結果の確認、構成管理システム使用の確認、開発者環境の確認、開発者による誤使用分析
EAL2	Structurally tested	サブシステムレベルまでセキュリティ機能設計の確認、構成管理の確認、開発者による機能強度、脆弱性分析、評価者による侵入テスト
EAL1	Functionally Tested	セキュリティ機能仕様、マニュアルの確認、評価者による

プロジェクトの例

対象	開発企業	形式手法
EAL6プロジェクト		
Trusted Services Engine (TSE)	galois(米) DoD(米)	HOL
Block Access Controller (BAC)	galois(米)	HOL
EAL5プロジェクト		
スマートカードOS	Gemplus(仏)	B
バイオメトリクス認証システム(TIS)	Praxis HIS(英) NSA(米)	SPARK, Z
EAL4プロジェクト		
Felicaチップ	Felica Networks(日)	VDM

国際標準・業界標準等の形式手法適用状況:FIPS 140-2(暗号技術)

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

- FIPS 140-2(1999年11月公開)は、NIST(米国技術標準研究所)が策定した米国政府の連邦情報処理標準であり、暗号モジュール機器の暗号技術に関するセキュリティ要件を規定する。情報の重要度を4つに分類し、暗号モジュールが満たすべきセキュリティ・レベルを、レベル1からレベル4に分類する。レベル4で形式手法について言及している。

SECURITY LEVEL 4

In addition to the requirements for Security Levels 1, 2, and 3, the following requirements shall apply to cryptographic modules for Security Level 4.

·Documentation shall specify a formal model that describes the rules and characteristics of the cryptographic module security policy The formal model shall be specified using a formal specification language that is a rigorous notation based on established mathematics, such as first order logic or set theory.

• Documentation shall specify a rationale that demonstrates the consistency and completeness of the formal model with respect to the cryptographic module security policy.

• Documentation shall specify an informal proof of the correspondence between the formal model and the functional specification.

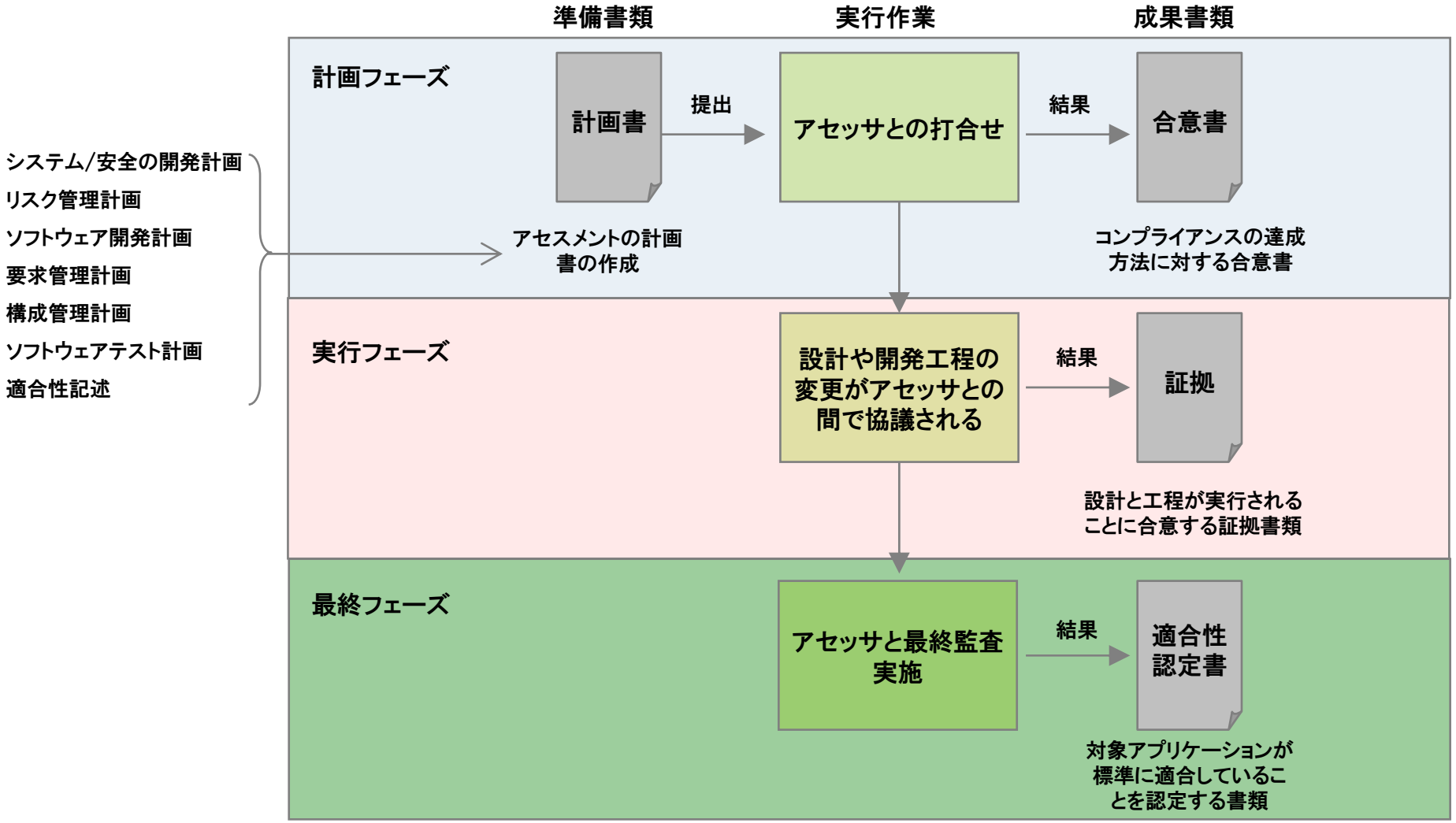
• For each cryptographic module hardware, software, and firmware component, the source code shall be annotated with comments that specify (1) the preconditions required upon entry into the module component, function, or procedure in order to execute correctly and (2) the postconditions expected to be true when execution of the module component, function, or procedure is complete. The preconditions and postconditions may be specified using any notation that is sufficiently detailed to completely and unambiguously explain the behavior of the cryptographic module component, function, or procedure.

• Documentation shall specify an informal proof of the correspondence between the design of the cryptographic module (as reflected by the precondition and postcondition annotations) and the functional specification.

参考：国際標準の認証：アセスメント手順

SEC
Software Engineering
for Mo・No・Zu・Ku・Ri

- 公開された標準であってもその内容には見方により解釈が異なることもある。従って、開発する対象が標準に準拠しているかの確認を得るためには、第3機関（アセッサ）による監査が必要となる。開発者は、開発の全工程にわたり標準に準拠していることを示す証拠を収集する必要がある。



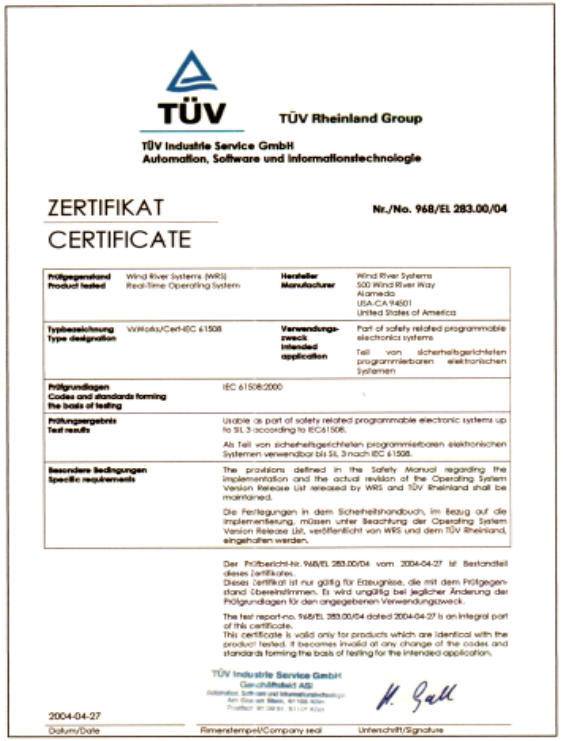
参考：国際標準の認証：ソフトウェア（ツール、RTOS）の例

- ISO/IEC 61508のSIL3の認証を受けたRTOSとして、Wittenstein high integrity systems社のSafeRTOS（英）、GreenHills社のNTEGRITY/velOSity、WindRiver社のVxWorksがあり、いずれもTÜVのアセスメントを受け認証を得ている。ツールの例では、Esterel社（仏）のSacde Code Generetor KCG がSIL3とEN50128の認証（SIL3/4）を得ている。
- 認証を受けたソフトウェア（OSやツール）をシステムの開発に使用することで、開発対象のシステムが同等の認証を受けられるわけではない。しかし、認証を受けたソフトウェアが認証過程で集めたSIL3準拠を示す証拠を、開発対象システムがSIL3の認証を得る際の証拠とすることができる。
- 認証RTOSを使用することで、開発対象システムのSIL3 を得るための分析や評価が必要なくなるわけではない。のこのためRTOSは認証のために必要なテストの手順やテストツールなどからなる「認証パック」をユーザに提供している。

Scade Code Generator KCG(Esterel)

INTEGRITY/velOSity(GreenHills)

VxWorks(WindRiver)



政府・公共調達等における形式手法適用状況

SEC
Software Engineering
for Mo・No・Zu・Ku・Ri

- WTO政府調達協定：GPA（The Agreement on Government Procurement）
  - WTOの規定では政府が購入する製品やサービスは国際標準や国内の技術規制に従い調達することを規定
  - 形式手法適用の製品やサービスの購入につて直接規定するものではない
  - しかし、「国際標準に従う」ことは、先に述べた ISO/IEC 61508などの形式手法の採用を記載する標準に沿った政府調達をすることを規定していると言える。

> 条項4：技術仕様
>
> 2. 調達部門は、適宜、技術仕様を：
>
> (a)デザインや記述的特徴よりむしろ性能の観点で規定すべき
>
> (b)国際標準があるならば、それに基づき、ないならば、国内標準として認識される国内の技術規定あるいは、建築基準法に基づき規定すべきである。

- 英国軍事調達：Def Stan 00-55
  - Def Stan 00-55（REQUIREMENTS FOR SAFETY RELATED SOFTWARE IN DEFENCE EQUIPMENT）では、英国の軍事調達において安全系ソフトウェアを購入する場合の形式手法の適用について規定している。

> 0.3 Assurance that the required safety integrity has been achieved is provided by the use of formal methods in conjunction with dynamic testing and static analysis. A Software Safety Case, which justifies the suitability of the software development process, tools and methods, is required for software of all integrity levels. This Software Safety Case contributes to and forms part of the equipment safety case required by Def Stan 00-56.

政府・公共調達等における形式手法適用状況

SEC
Software Engineering
for Mo・No・Zu・Ku・Ri

- 米国国家情報保証調達ポリシー(National Information Assurance Acquisition Policy) (2000 年1月発行)
  - 国防総省が議長を務める国家安全保障通信・情報システムセキュリティ委員会(NSTISSC)、現在の国家セキュリティシステム委員会(CNSS)、によって策定された、情報保証(Information Assurance：IA)とIA対応のIT 製品の調達に関する方針の規定

連邦政府が調達する民生品(COTS)に関して、以下の制度に従うべきことを規定する。

CCEVS(Common Criteria Evaluation and Validation Scheme)制度:
IT製品がISO/IEC15408(コモンクライテリア)に適合する評価・認証を行うプログラム

CMVP(Cryptographic Module Validation Program):
FIPS 140-2(連邦情報処理標準)に基づく、暗号モジュール評価、認証プログラム
FIPS 140-2には形式手法について記述がある。

NPIVP(NIST Personal Identity Verification Program):
PIVカードアプリケーション、PIVカードミドルウェアの認定制度、PIVカードとは、連邦政府職員及び契約業者の個人識別カード

連邦政府機関が情報セキュリティ関連製品および、暗号モジュール関連製品を調達する場合以下の制度により認定された製品を選ぶことを規定する。

CMVP (Cryptographic Module Validation Program) :
FIPS 140-2 (連邦情報処理標準) に基づく、暗号モジュール評価、認証プログラム
FIPS 140-2では形式手法について記述がある。

Cryptographic Module Testing (CMT)により認定された製品、あるいはCCEVS の基で実施される検査制度

Common Criteria Testing (CCT)

IPA Software Engineering Center
Information-technology Promotion Agency, Japan

2010年7月29日

独立行政法人　情報処理推進機構
ソフトウェア・エンジニアリング・センター