

as Wing
Infinity
by Trusty
technology
om Zero

日本初 機能安全規格 IEC 61508 SIL 3 に準拠した リアルタイムOSを一般公開に

～戦略的基盤技術高度化支援事業の成果を活用～



株式会社ヴィッツ
服部博行

株式会社ウィッツは、国際認証機関 TÜV SÜD より、機能安全規格 IEC 61508 SIL3 開発が可能なソフトウェアプロセス認証を取得し、そのプロセスを用いて、国内で初めて IEC 61508 SIL3 Capable のリアルタイムOS開発に成功しました



ウィッツが開発した機能安全OS

- 開発した機能安全OS = リアルタイムカーネル + 故障検出ライブラリ
 - カーネルと故障検出ライブラリは
SIL3 開発プロセスを適用
カーネルはTOPPERS/ASP のサブセット
 - 故障検出率90%を実現する検出ライブラリ

機能安全 OS =



- 機能安全OS を用いたシステムに対して、**故障検出率が90%以上の診断機能**を提供可能。
JIS C0508-2より抜粋

自己診断率	ハードウェアフォールトトレランス(備考2.参照)		
	0(備考3.参照)	1	2
なし(0%)	許可されない	SIL1	SIL2
低(60%)	SIL1	SIL2	SIL3
中庸(90%)	SIL2	SIL3	SIL4
高(99%)	SIL3	SIL4	SIL4

マイコンが、1重系:SIL2、2重系:SIL3 を実現可能



2010/12/24
TOPPERS会員向け早期リリース
2011/3/E 一般公開

アプリケーション

リアルタイムカーネル
故障検出ライブラリ

R32C/133



2011/3/E
一般販売

IEC 61508 SIL3 Capable Realtime Kernel

⇒ TOPPERS/ASP Safety

提供形態: オープンソース公開

- ・Kernel Source code
- ・Safety Concept
- ・Safety Requirement
- ・Safety Manual etc.

故障検出等はアプリケーションで実施する

TOPPERS/ASP Safety + 故障検出ライブラリ

⇒ Owls Safety Package

提供形態: 販売

- ・機能安全認証に必要なすべてのドキュメント
- ・Kernel, 故障検出ライブラリのソースコード一式

IEC61508 が要求する故障検出率90%を故障検出ライブラリで実現可能。

Owls 故障検出ライブラリ



コンポーネント	故障検出ライブラリ	DC	起動時	実行中
電気・電子サブシステム	対象外 (ユーザが必要に応じて対応する必要あり)	—	—	—
I/O、電源	対象外 (ユーザが必要に応じて対応する必要あり)	—	—	—
バス	ROM故障検出機能	99%	○	○
	RAM故障検出機能	90%	○	○
CPU	CPU故障検出機能	90%	○	×
	実行シーケンスモニタ機能		×	○
	W/Dタイマ故障検出機能		○	×
割込みハンドリング	割込みコントローラ故障検出機能	90%	○	×
ROM	ROM故障検出機能	99%	○	○
RAM	RAM故障検出機能	90%	○	○
クロック	実行シーケンスモニタ機能	90%	×	○
通信、大規模ストレージ	対象外 (ユーザが必要に応じて対応する必要あり)	—	—	—
センサ	対象外 (ユーザが必要に応じて対応する必要あり)	—	—	—
アクチュエータ	対象外 (ユーザが必要に応じて対応する必要あり)	—	—	—

本認証取得に際し、経済産業省・(独)中小企業基盤整備機構の戦略的基盤技術高度化支援事業の採択テーマとして実施した「機能安全対応自動車制御プラットフォームの開発」の成果を活用しました。

研究実施プロジェクトのメンバならびにアドバイザー各位

メンバ組織

(株)ヴィッツ、(株)サニー技研、東海ソフト(株)

名古屋大学(NCES)、産業技術総合研究所(CVS)

名古屋市工業研究所、北海道立工業試験場

アドバイザー組織

トヨタ自動車(株)、アイシン精機(株)、(株)東海理化、アイシン・エイ・ダブリュ(株)、(株)ルネサステクノロジ、(株)豊通エレクトロニクス、筑波大学

OSの一般販売を開始



Owls Industrial Package

μITRON仕様 OS



Owls AUTOSAR Package

AUTOSAR R3.x OS



Owls Automotive Package

OSEK/VDX OS

全シリーズ 機能安全パッケージと保護機能パッケージを準備

(一部準備中)

本発表への問い合わせ先

一般公開物および製品等のより詳しい内容は、ET2010展示場内 E28 TOPPERSパビリオン内のウィッツブースまでお越しください

総合問い合わせ先

株式会社ウィッツ

総務部: 安場、佐藤 (052) 220-1218

技術的問い合わせ先

株式会社ウィッツ

技術本部: 服部(hat@witz-inc.co.jp)

森川(morikawa@witz-inc.co.jp)

(052) 223-7570

ご静聴ありがとうございました

本内容についてのご質問は下記にお願いします

株式会社ヴィッツ

Tel: 052-220-1218

服部博行

hat@witz-inc.co.jp