

JEITA 組込み系ソフトウェア・ワークショップ2010

# 発電監視制御システムにおける プロダクトライン構築事例

2010年10月29日

株式会社 東芝 電力システム社  
原子力プロセス監視制御システム部  
小田川 直人



東芝グループは、持続可能な  
地球の未来に貢献します。

# 目 次

---

- 1. ソフトウェアプロダクトラインとSPL殿堂**
- 2. 発電監視制御計算機システムの概要**
- 3. プロダクトラインの構築(プラント自動化機能の例)**
- 4. ソフトウェアプロダクトラインとしての特徴**

SPL : Software Product Line

# 目 次

---

## 1. ソフトウェアプロダクトラインとSPL殿堂

## 2. 発電監視制御計算機システムの概要

## 3. プロダクトラインの構築(プラント自動化機能の例)

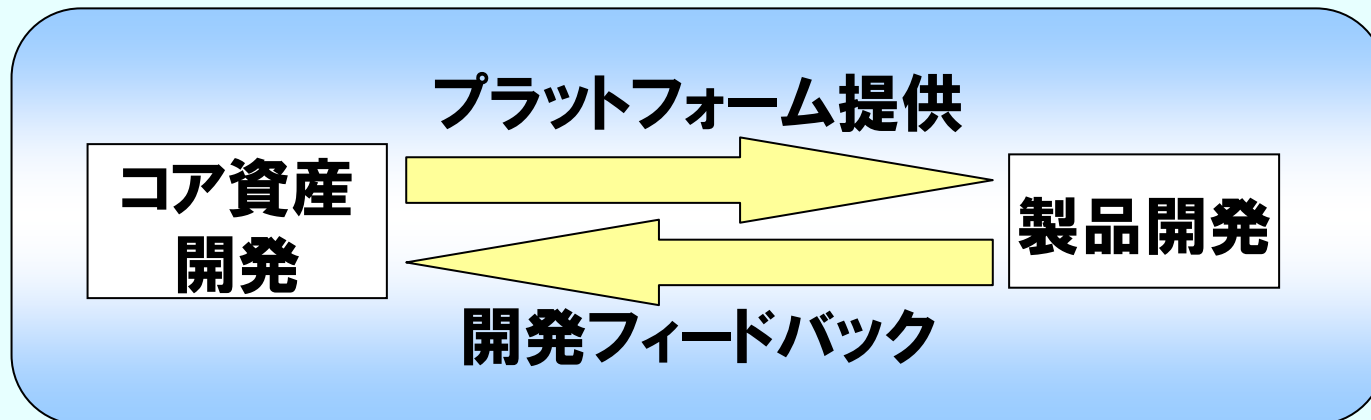
## 4. ソフトウェアプロダクトラインとしての特徴

# 1.1 ソフトウェアプロダクトラインとは

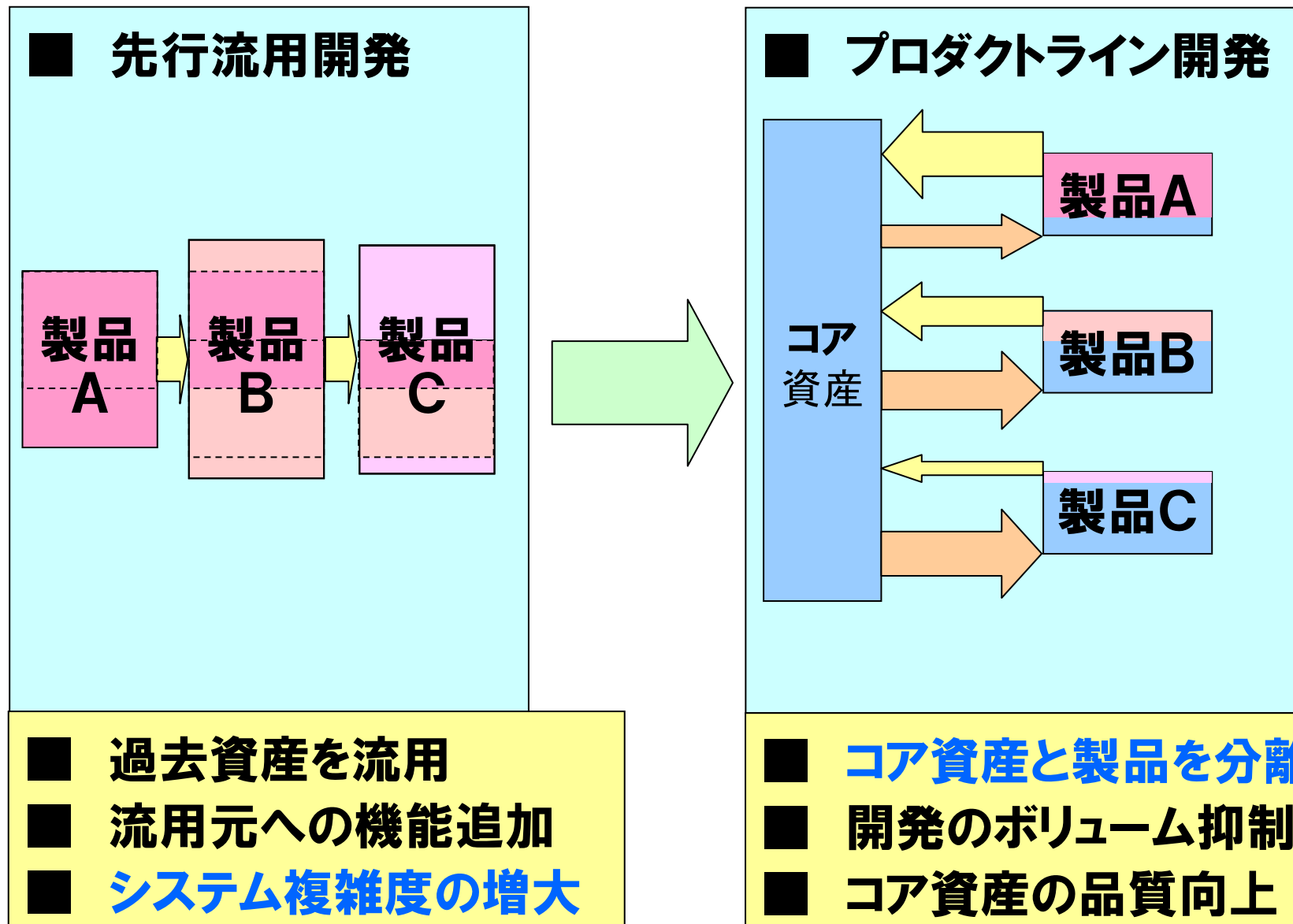
## ■ CMU/SEI(※)の定義 ※CMU/SEI:カーネギーメロン大学ソフトウェア工学研究所

- 管理されたソフトウェア集約型システムの集合
- 共通のコア資産を元に作られる
- 特定の市場分野の要求を満たす。

## ■ 具体的説明



# 1.2 ソフトウェアプロダクトラインによる製品開発



## 1.3 ソフトウェアプロダクトライン殿堂入り

- 弊社発電監視制御システムが、SPLC2008にてソフトウェアプロダクトラインの殿堂に登録“Software Product Line Hall of Fame”

[www.splc.net/fame/toshiba.html](http://www.splc.net/fame/toshiba.html)

### ■ 評価ポイント

- **DSL構築とコア資産化**によるプロダクトライン構築  
(プラント固有部と標準部を明確に分離)
- **基本コンセプトを維持したシステム開発**  
(基本コンセプトを維持し、ハード/OS/構成の変化に対応したシステムを構築)
- **事業的成功** (150システム以上の出荷実績)
- **学術的貢献** (69件(英語のみ)の論文発表)

DSL:Domain Specific Language(ドメイン固有言語)

# 1.4 ソフトウェアプロダクトライン殿堂入り

企業名	国名	プロダクトラインの対象
Hewlett Packard	アメリカ	プリンタ、コピー、スキャナのファームウェア
NOKIA	フィンランド	携帯電話ソフトウェア
Celsius Tech	スウェーデン	船舶制御システム
US Naval Research Laboratory	アメリカ	飛行機パイロットの運行支援システム
MARKE MAKER Software AG	ドイツ	Webシステムソフトウェア
Boeing	アメリカ	軍用機のパイロット支援システム
AT&T Bell Labs/Lucent Technology	アメリカ	電話交換機ソフトウェア
Philips	オランダ	電話交換機ソフトウェア
Cummings, Inc.	アメリカ	ディーゼルエンジン制御ソフトウェア
Philips	オランダ	TV向け組み込みソフトウェア
Salion, Inc.	アメリカ	資金管理システム
Ericsson	スウェーデン	電話交換機ソフトウェア
General Motors	アメリカ	自動車制御組み込みソフトウェア
LIS Logic	アメリカ	RAID制御ファームウェア
Bosch	ドイツ	ガソリンエンジン制御ソフトウェア
Philips	オランダ	医療システム
東芝	日本	発電監視制御システム

# 目 次

---

## 1. ソフトウェアプロダクトラインとSPL殿堂

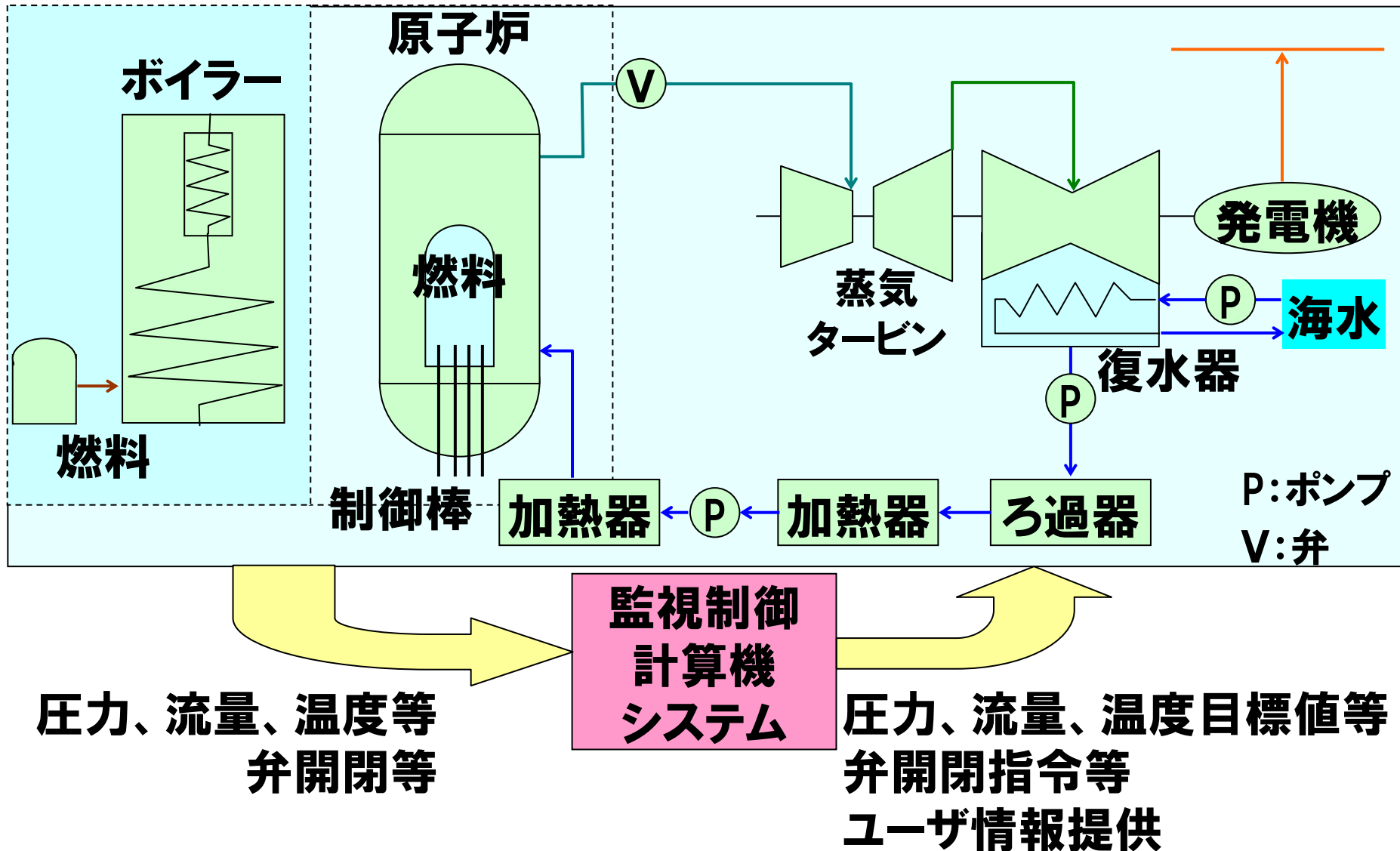
## 2. 発電監視制御計算機システムの概要

## 3. プロダクトラインの構築(プラント自動化機能の例)

## 4. ソフトウェアプロダクトラインとしての特徴



## 2.1 発電プラントの概要



## 2.2 発電監視制御計算機システムの特徴

### ■ システム要求

- 設計着手からシステム稼働までが長期間(2~5年)
- 多数の入出力点数の高速処理(接点1ms、アナログ10ms)
- 長期保守(稼働後10~15年)
- 高安全性、高品質、トレーサビリティ

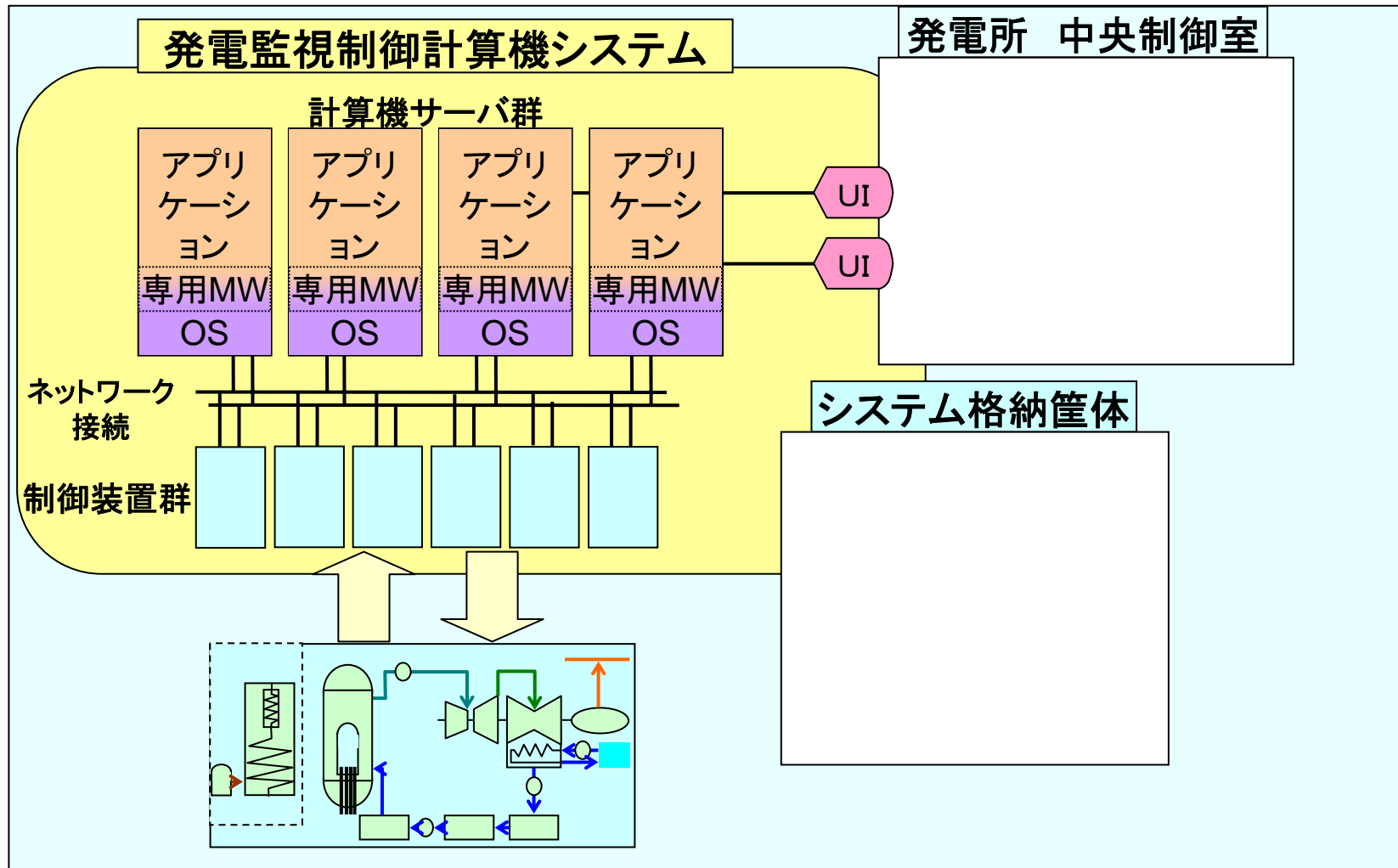
### ■ 製品の特徴

- プラントの違い、顧客運用の差異の機能への反映
- 実プラント挙動への柔軟な対応
- ハードウェア/OS変更への柔軟な対応

開発効率・保守効率を上げる仕組みを構築

ソフトウェアプロダクトラインの実現

## 2.3 発電監視制御計算機システム構成例



UI: ユーザーインターフェイス  
MW: ミドルウェア

## 2.4 発電監視制御計算機システムの変遷

	1960年代	1970年代	1980年代	1990年代	2000年代
表示形態		キャラクター表示	セミグラフィック	フルグラフィック	
システム構成		一重系	二重化	機能分散	水平分散
監視形態		集中システム		分散システム	

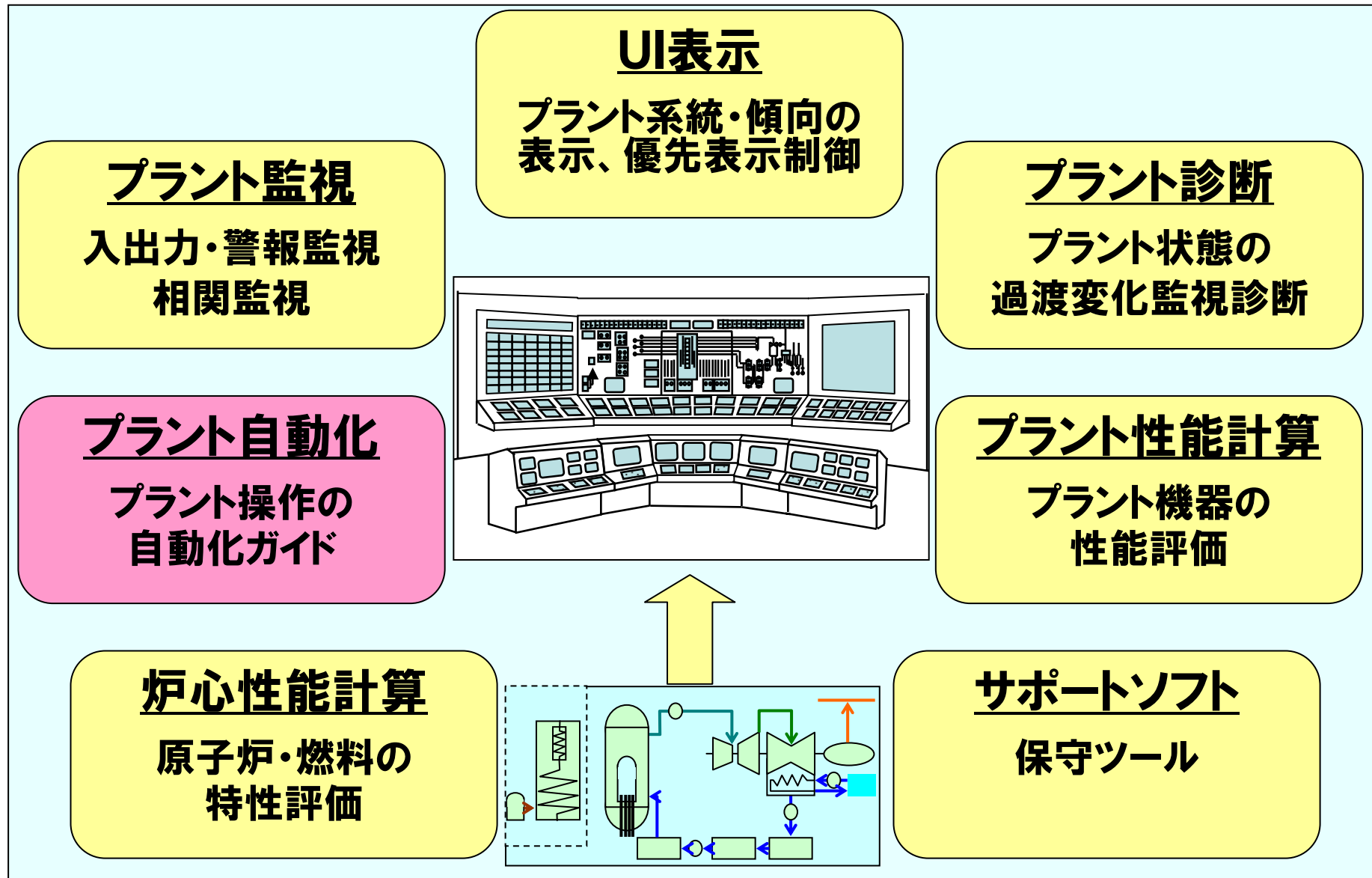
■ OS/ハードの変化に応じたソフトウェア開発

### 最近のシステム規模(原子力)

サーバ: 50台  
表示画面: 700枚

入出力点数: 24000点  
アプリソフト: 300万ステップ  
DSL: 1.5GByte

## 2.5 発電監視制御計算機システムの機能



# 目 次

---

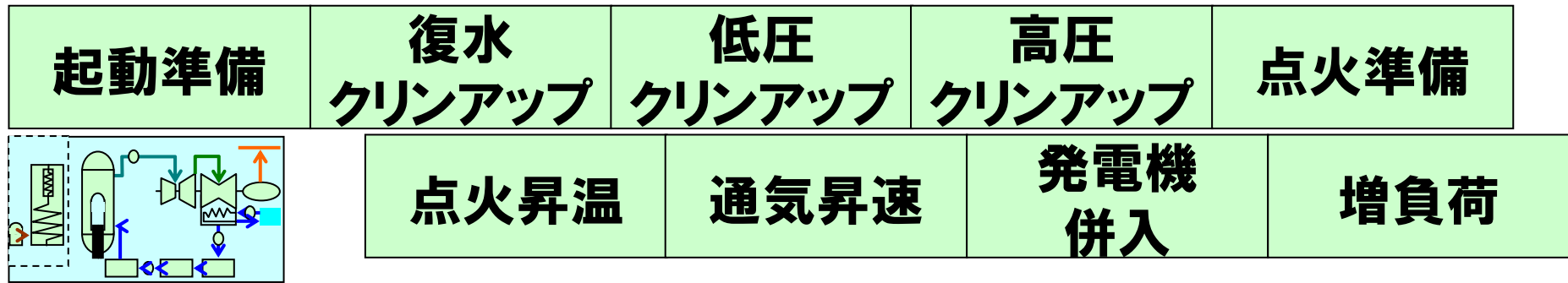
## 1. ソフトウェアプロダクトラインとSPL殿堂

## 2. 発電監視制御計算機システムの概要

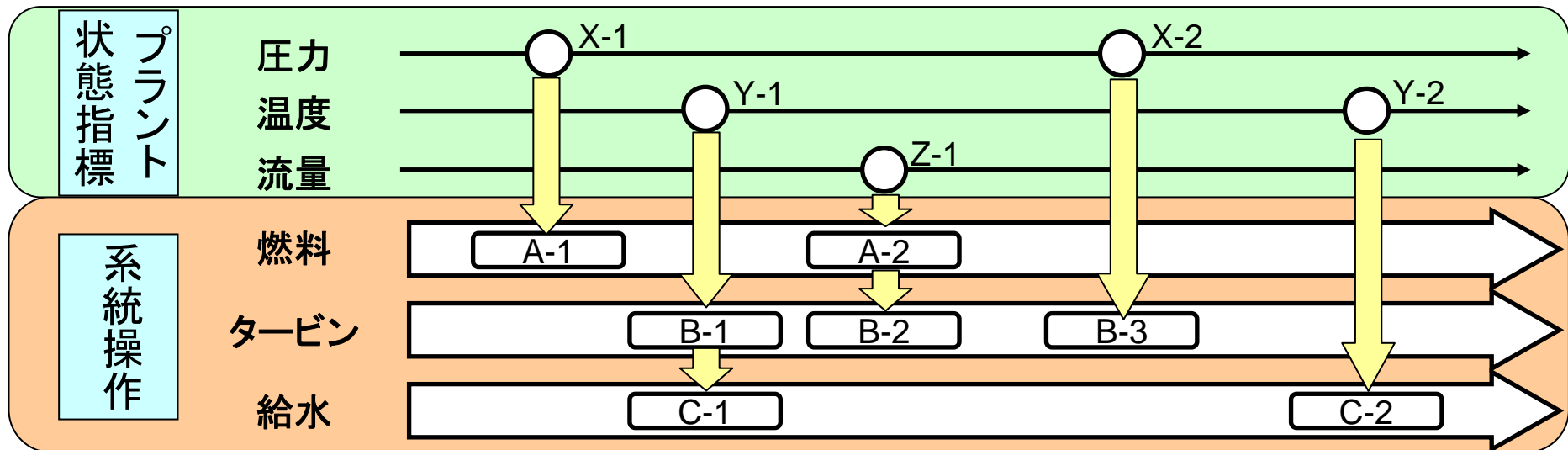
## 3. プロダクトラインの構築(プラント自動化機能の例)

## 4. ソフトウェアプロダクトラインとしての特徴

# 3.1 プラント自動化機能の概要



- 発電プラントの複雑な起動／停止、通常運転の操作
- 起動、停止目標の計算、条件判定
- 異常時の定型操作



## 3.2 プラント自動化機能の歩み(1)

- 多段階の操作が必要
- 多数の入力、系統の処理が必要

- プラント運転員の  
負荷大

### プラント制御の計算機による自動処理 (プラント自動化機能)

#### ■ 開発当時の世の中の状況

##### 米国で試みるも動かず

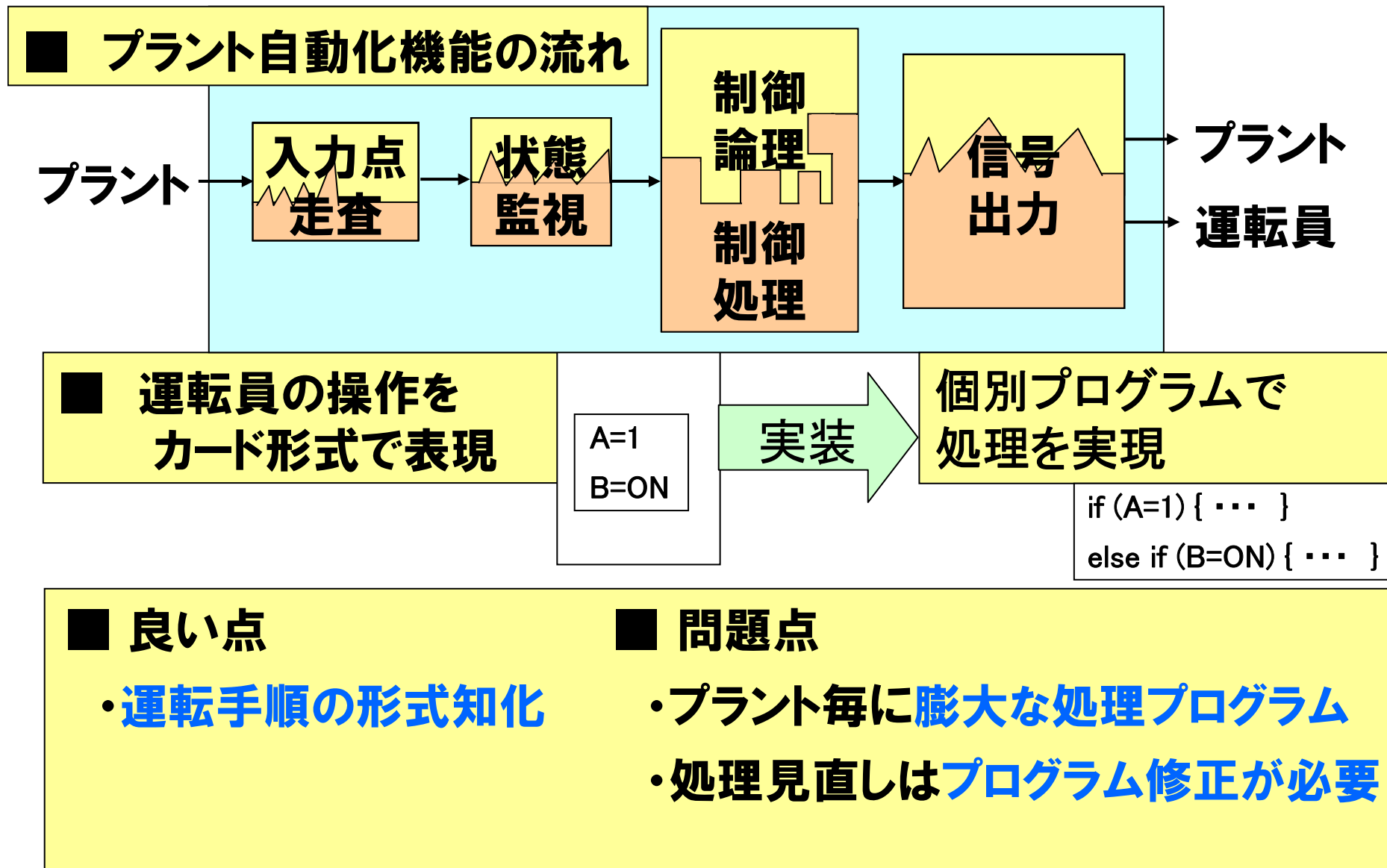
- 1960 ハンテントンビーチ
- 1961 リトルジブシー
- 1965 マウンテンリーク
- 1971 ピッツバーグ

- ・計画は意欲的
- ・失敗の連続
- ・商用化できず

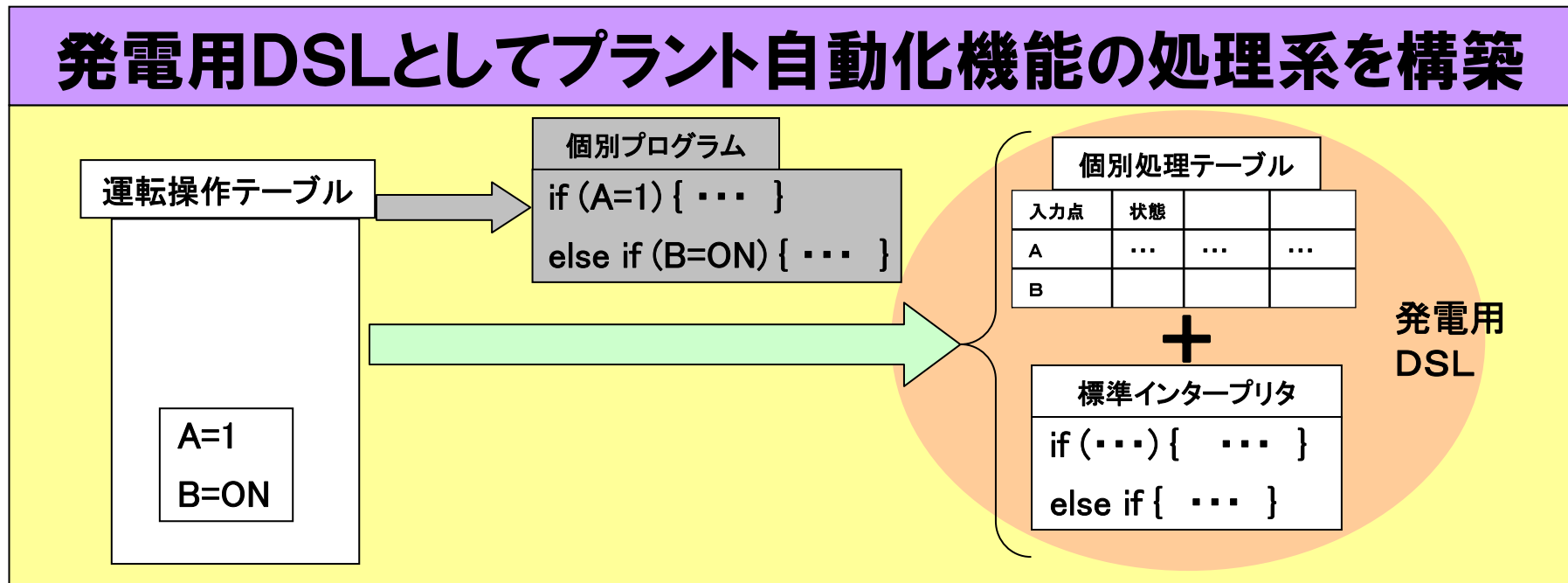
計算機的能力不足、信頼性不足  
ソフトウェアの開発環境が未整備



### 3.3 プラント自動化機能の歩み(2)



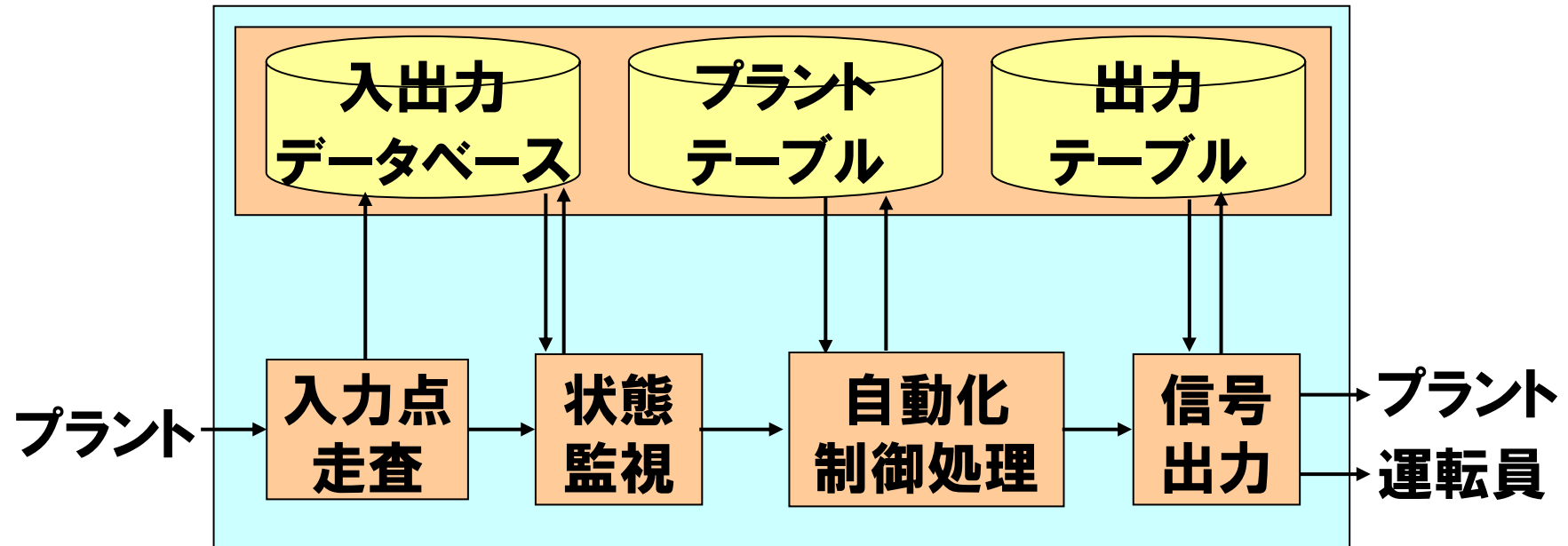
### 3.4 プラント自動化機能の構築(1)



入出力情報	入出力点情報の記述
運転タイミング情報	運転タイミングを入力点情報を用いて記述
操作タイミング管理情報	操作が動作するタイミングの記述
多重条件情報	共通条件の記述
操作情報	操作内容の記述

## 3.5 プラント自動化機能の構築(2)

### 発電用DSLとしてのプラント自動化機能

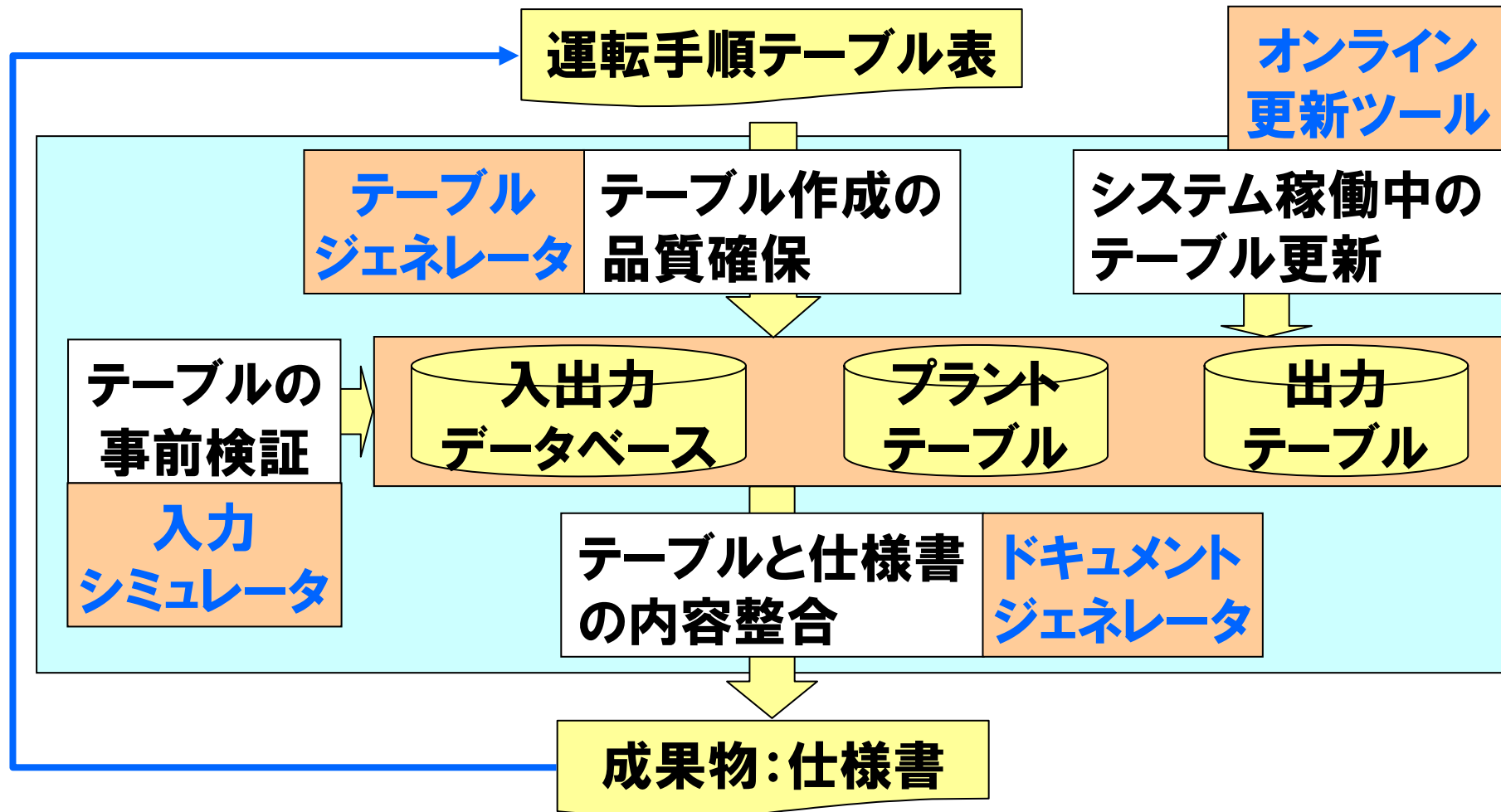


- **制御処理の標準化**  
全プラント共通で管理(コア資産)
- **制御論理のテーブル化**  
テーブルはプラント知識のみ  
2000~5000枚/プラント

- **修正時はテーブルのみ変更**
- **テーブル変更手順の整備**  
プログラム技術者が不要

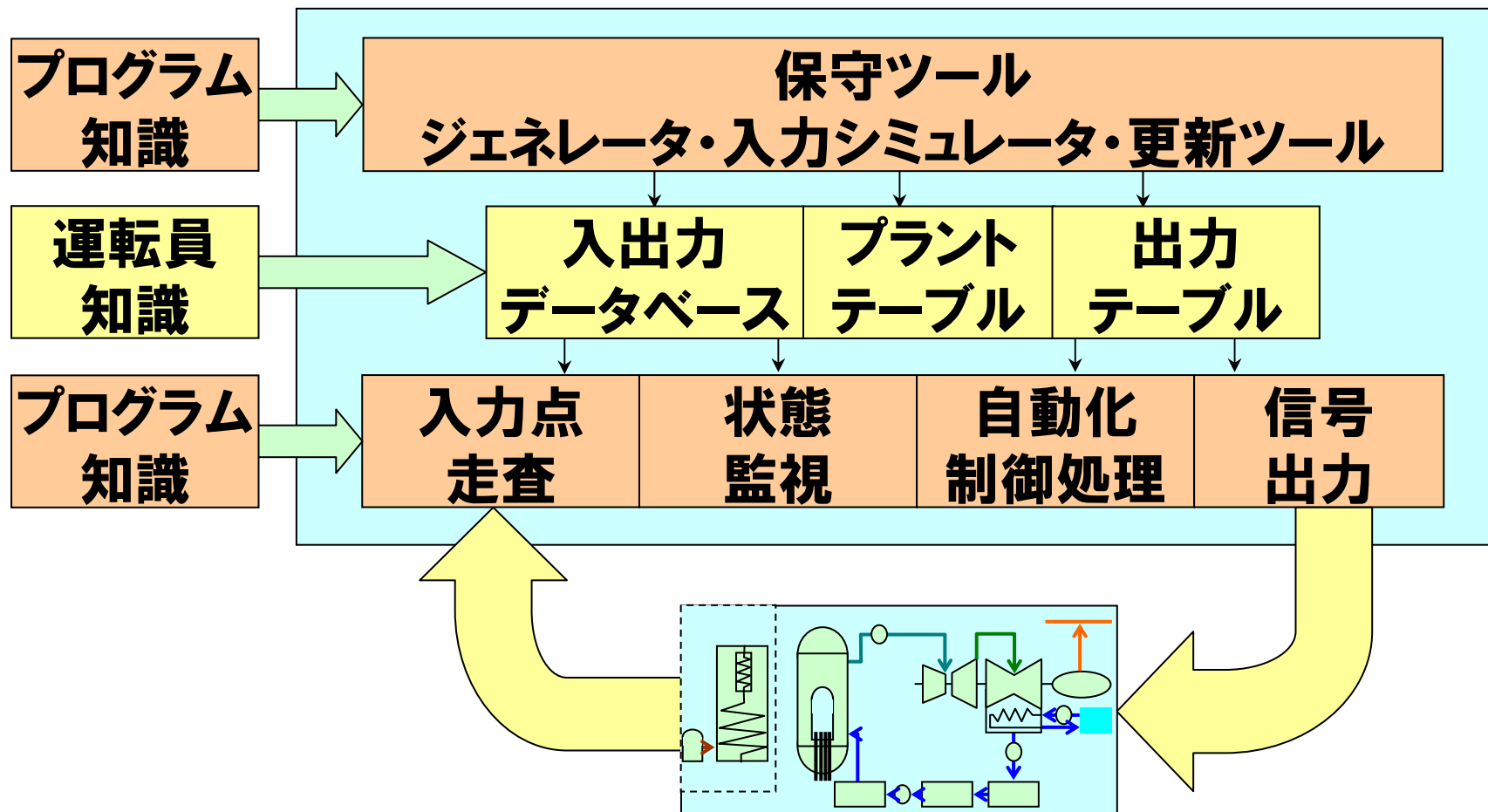
### 3.6 プラント自動化機能の構築(3)

#### 自動化用テーブル設計の品質・生産性向上



### 3.7 プラント自動化機能の構築(4)

世界初のプラント全自動化運転を実現



# 目 次

---

1. ソフトウェアプロダクトラインとSPL殿堂
2. 発電監視制御計算機システムの概要
3. プロダクトラインの構築(プラント自動化機能の例)
4. ソフトウェアプロダクトラインとしての特徴

# 目 次

---

## 4. ソフトウェアプロダクトラインとしての特徴

(1) ソフトウェアのコア資産化

(2) 自由度の高いシステム構築

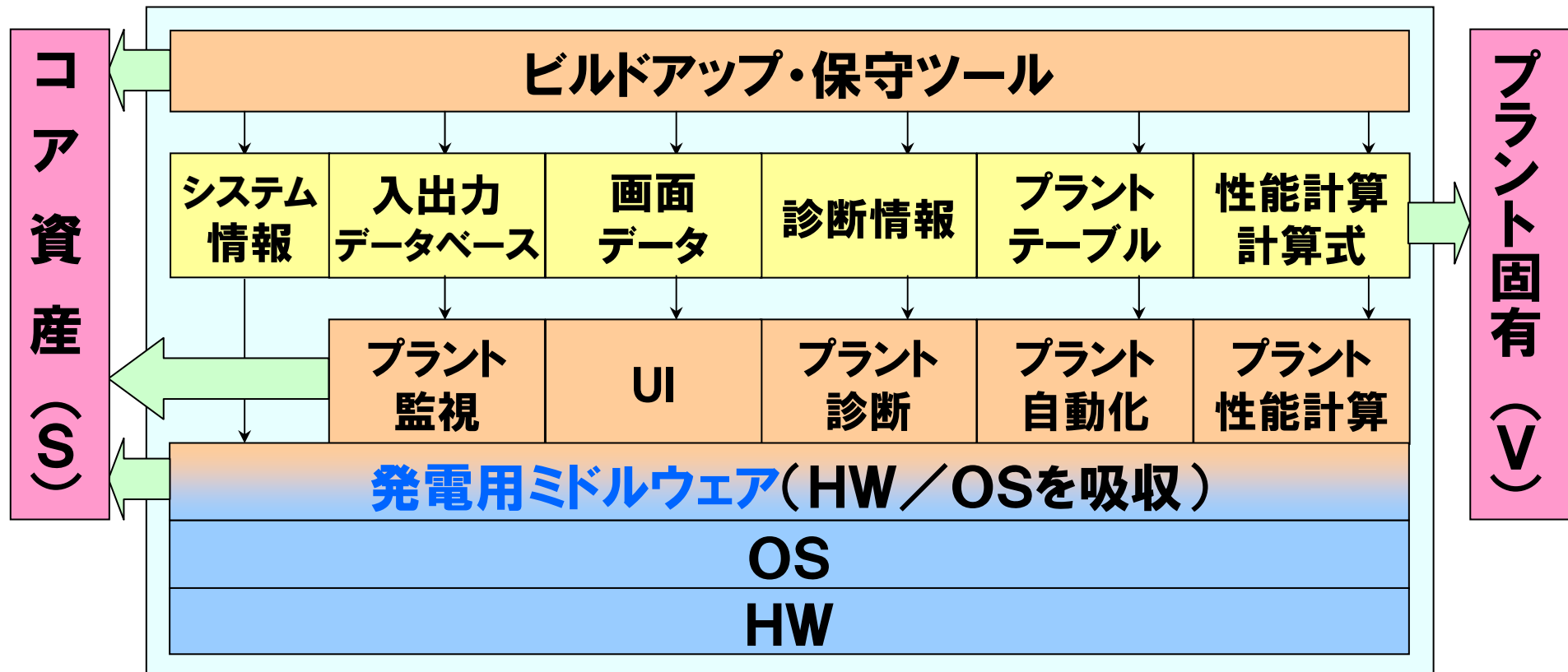
(3) プロダクトライン型開発工程

(4) コア資産の管理

# 4.(1) ソフトウェアのコア資産化

発電監視制御計算機システムの発電用DSL構築  
発電用DSLを用いたソフトウェアのコア資産化

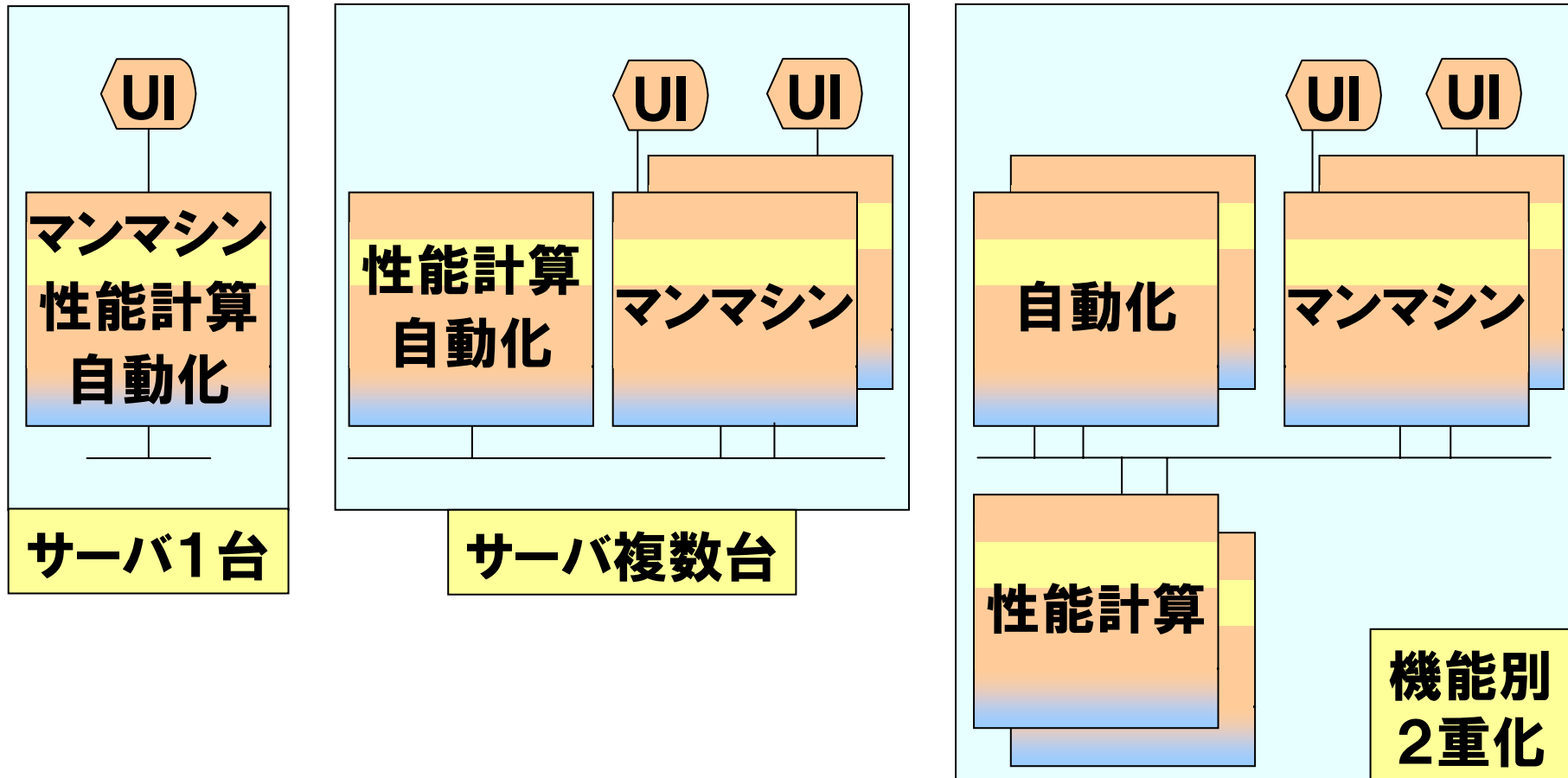
システムの徹底したS/V分離  
(コア資産 → Standard/プラント固有部 → Variable)





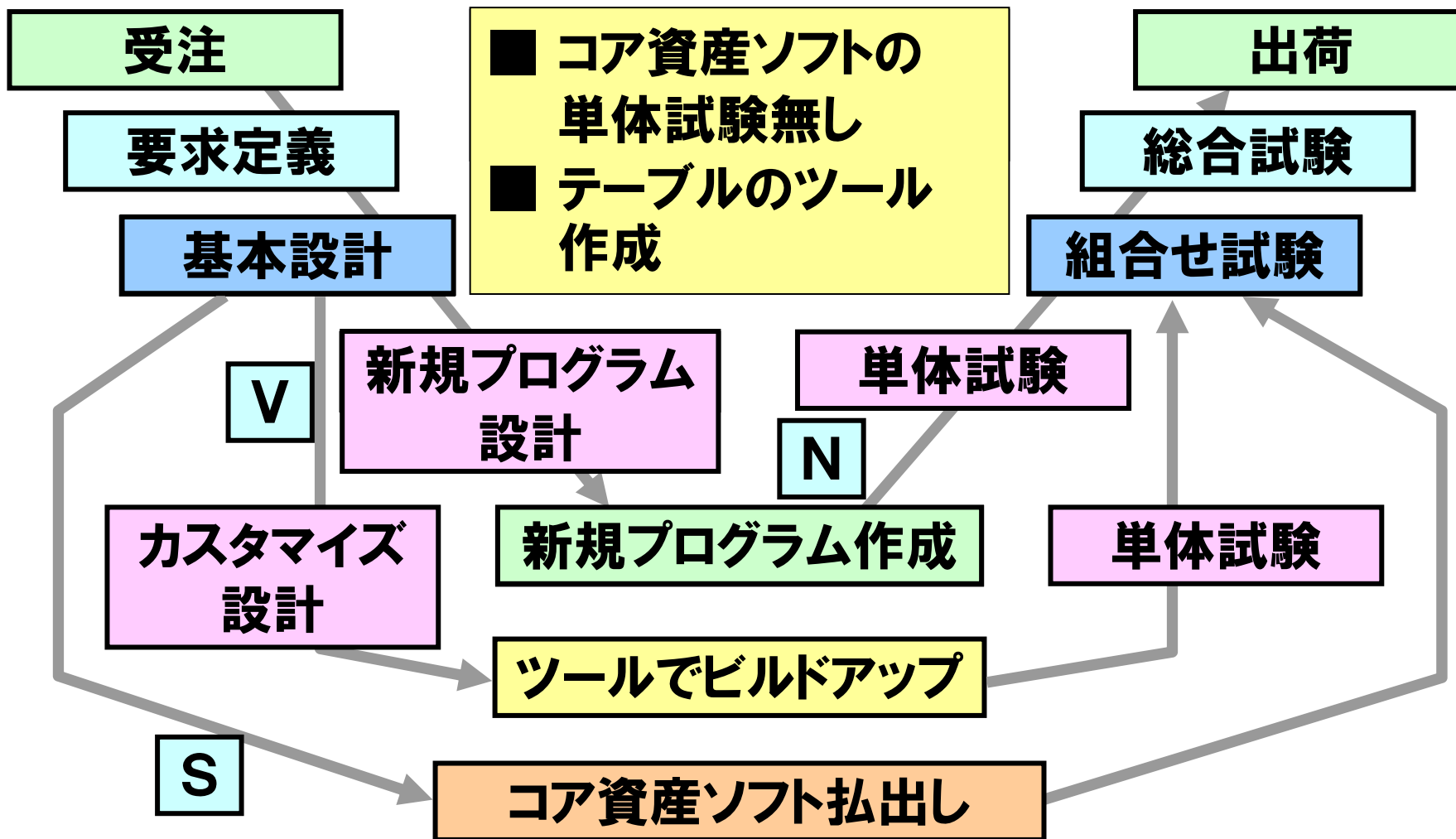
## 4.(2) 自由度の高いシステム構築

■ 単一のコア資産でサーバ1台構成から機能別2重化構成まで構築



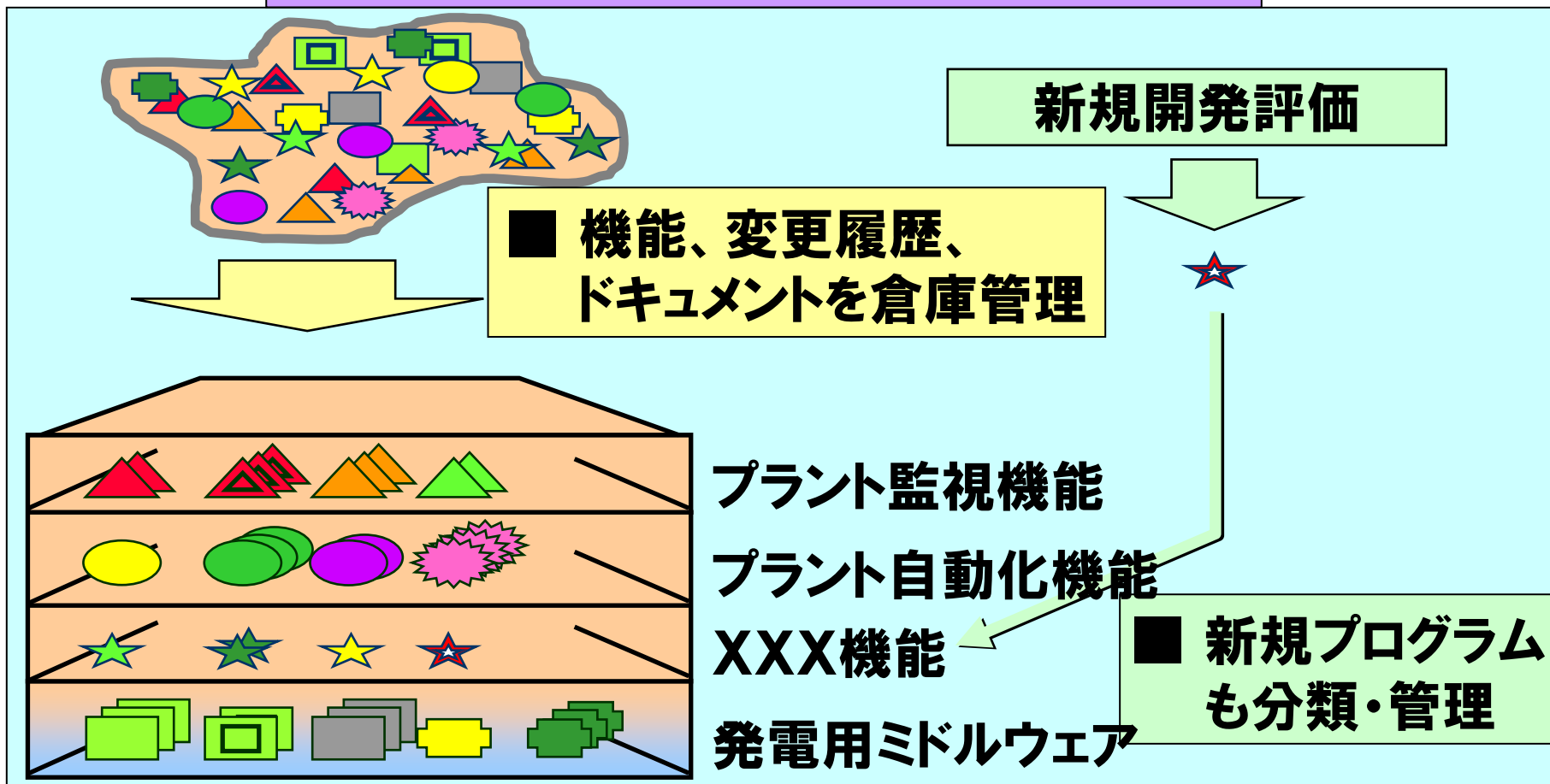
## 4.(3) プロダクトライン型開発工程

■ システム全体の品質・生産性向上



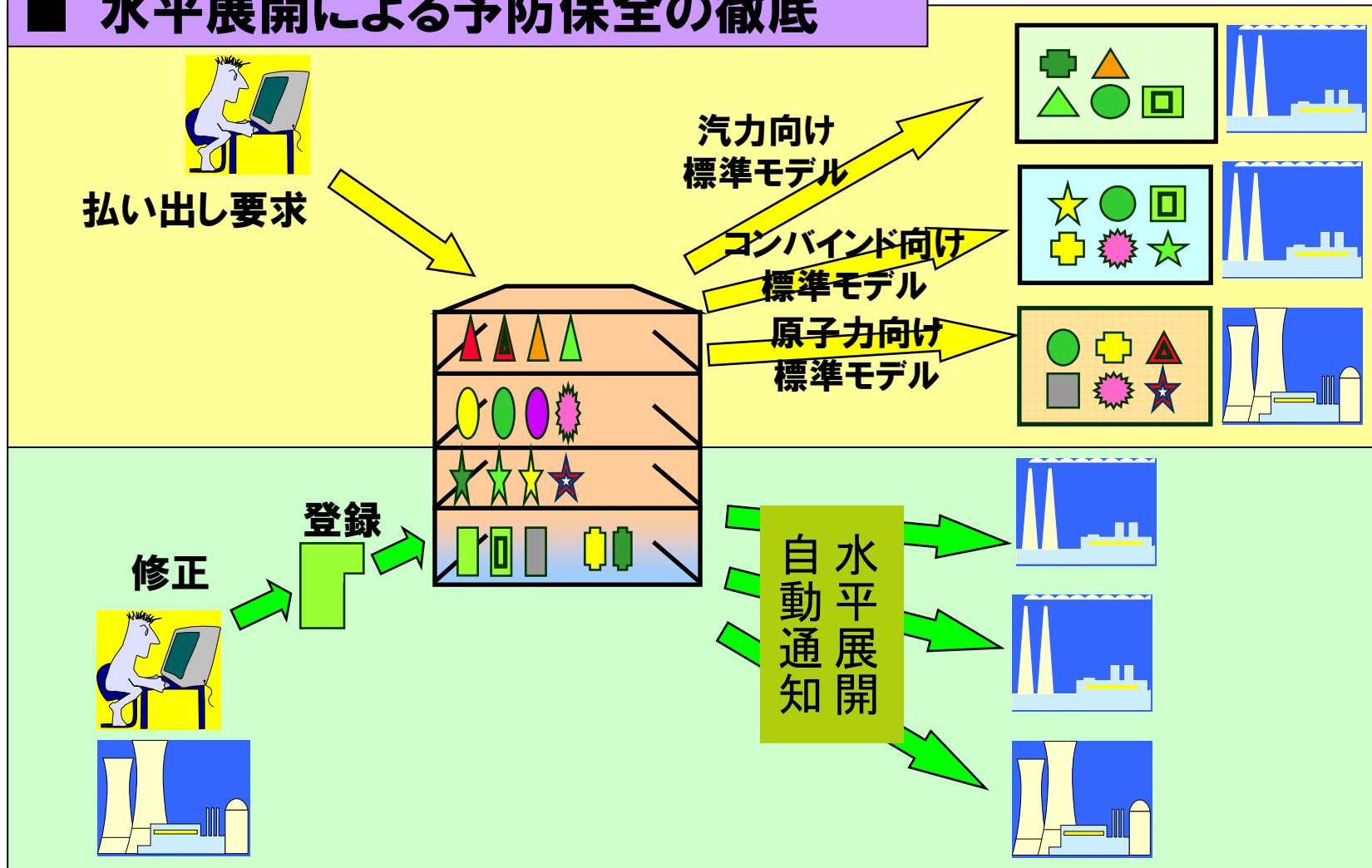
## 4.(4) コア資産の管理(倉庫管理)

- プログラムとドキュメントの管理
- 新規開発物量の評価
- 改造時の影響範囲の把握



## 4.(4) コア資産の管理(構成管理)

- 標準モデル構築による生産性向上
- 水平展開による予防保全の徹底



# まとめ

## ■ まとめ

- 発電監視制御計算機システムに、徹底したS/V分離によるプロダクトラインを構築
  - (DSL構築とコア資産化)
  - (プラント固有部と標準部を明確に分離)
  - (コア資産の管理体制の構築)
- 基本コンセプトを維持したシステム開発の継続
  - (基本コンセプトを維持し、ハード/OS/構成の変化に対応したシステムを構築)
  - (プログラム技術者不要のシステム開発)
- 事業的成功/学術的貢献

---

# **TOSHIBA**

## **Leading Innovation >>>**