MOVE THE WORLD FORWARD MITSUBISHI HEAVY INDUSTRIES GROUP

国立情報学研究所オープンハウス2024
産官学連携セミナー

重要インフラに対する形式手法に基づく高信頼性制御システムの開発事例

髙尾　健司

三菱重工業株式会社　総合研究所　知能化機械研究推進部


ガスタービン
市場シェア世界1位


CO_2回収プラント
市場シェア世界1位


ゴムタイヤ式
新交通システム
市場シェア国内1位


特殊車両


艦艇


ロケット


物流機器


ターボ冷凍機
市場シェア国内1位

Mitsubishi Heavy Industries, Ltd.

2024.06.07

MITSUBISHI HEAVY INDUSTRIES

目次

0. こんなところに三菱重工

1. 三菱重工のデジタルイノベーションブランドΣSynX

1. 三菱重工のデジタルイノベーションブランドΣSynX

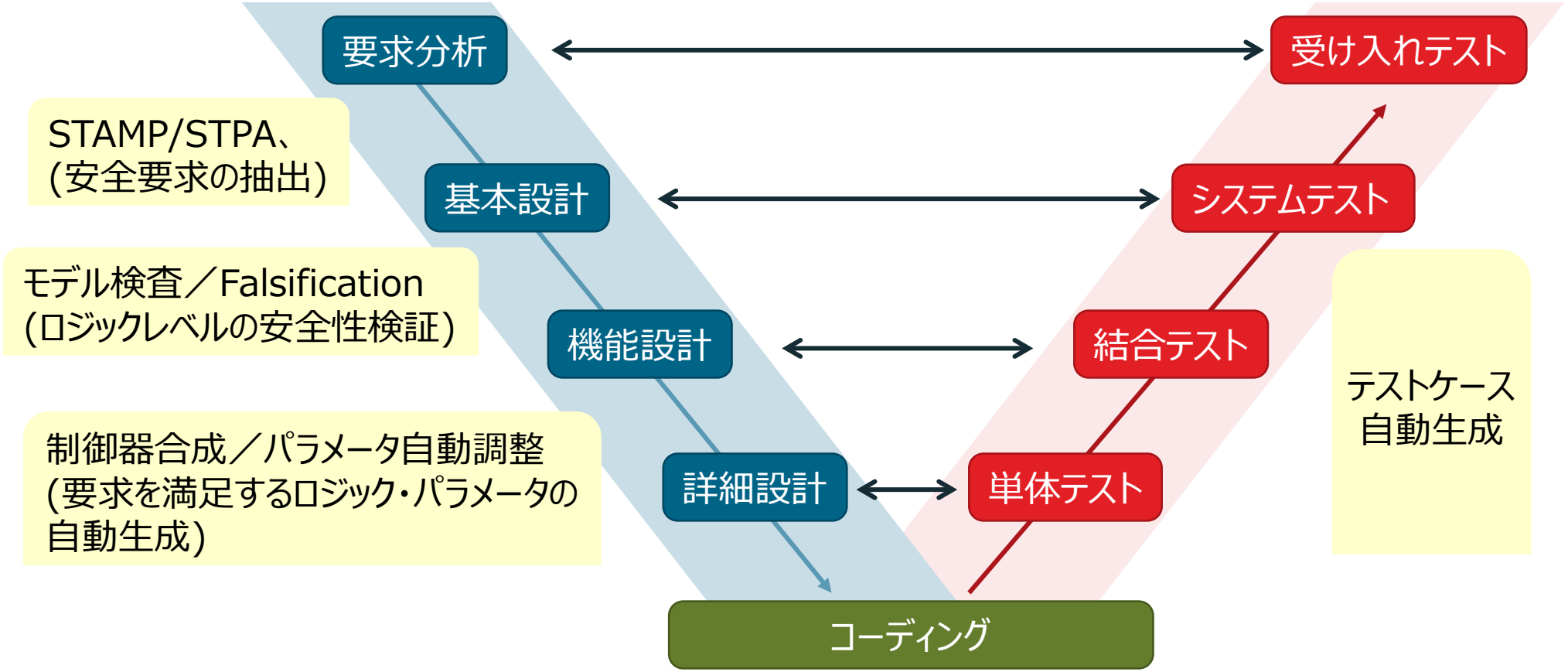
1. 三菱重工のデジタルイノベーションブランドΣSynX

高信頼性要求に応える自動検証技術・自動設計技術の研究開発

目次

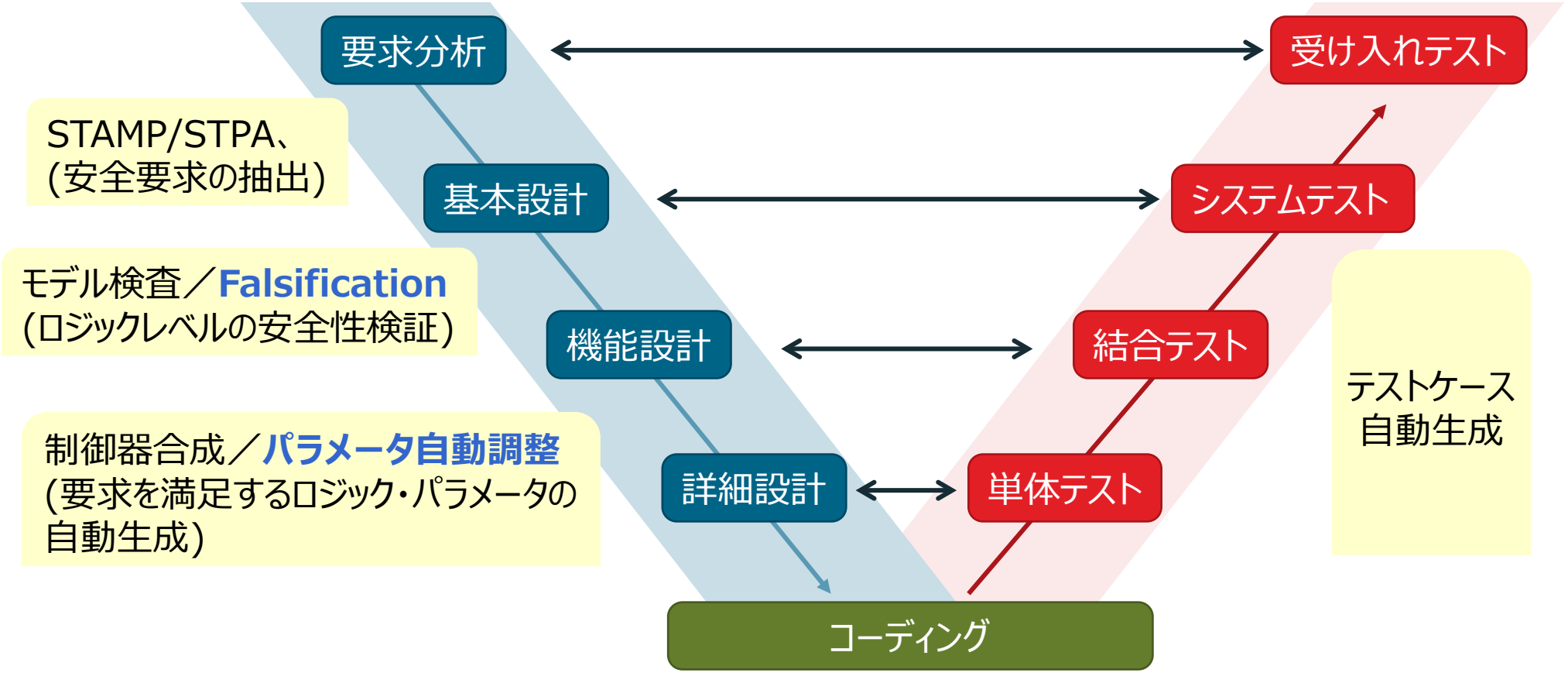
2. V字型開発プロセスと検証技術

三菱重工では開発プロセスの各フェーズに対応した検証技術を適用することで、
重要インフラ機器に要求される高い信頼性に応えています。



2. V字型開発プロセスと検証技術

三菱重工では開発プロセスの各フェーズに対応した検証技術を適用することで、
重要インフラ機器に要求される高い信頼性に応えています。



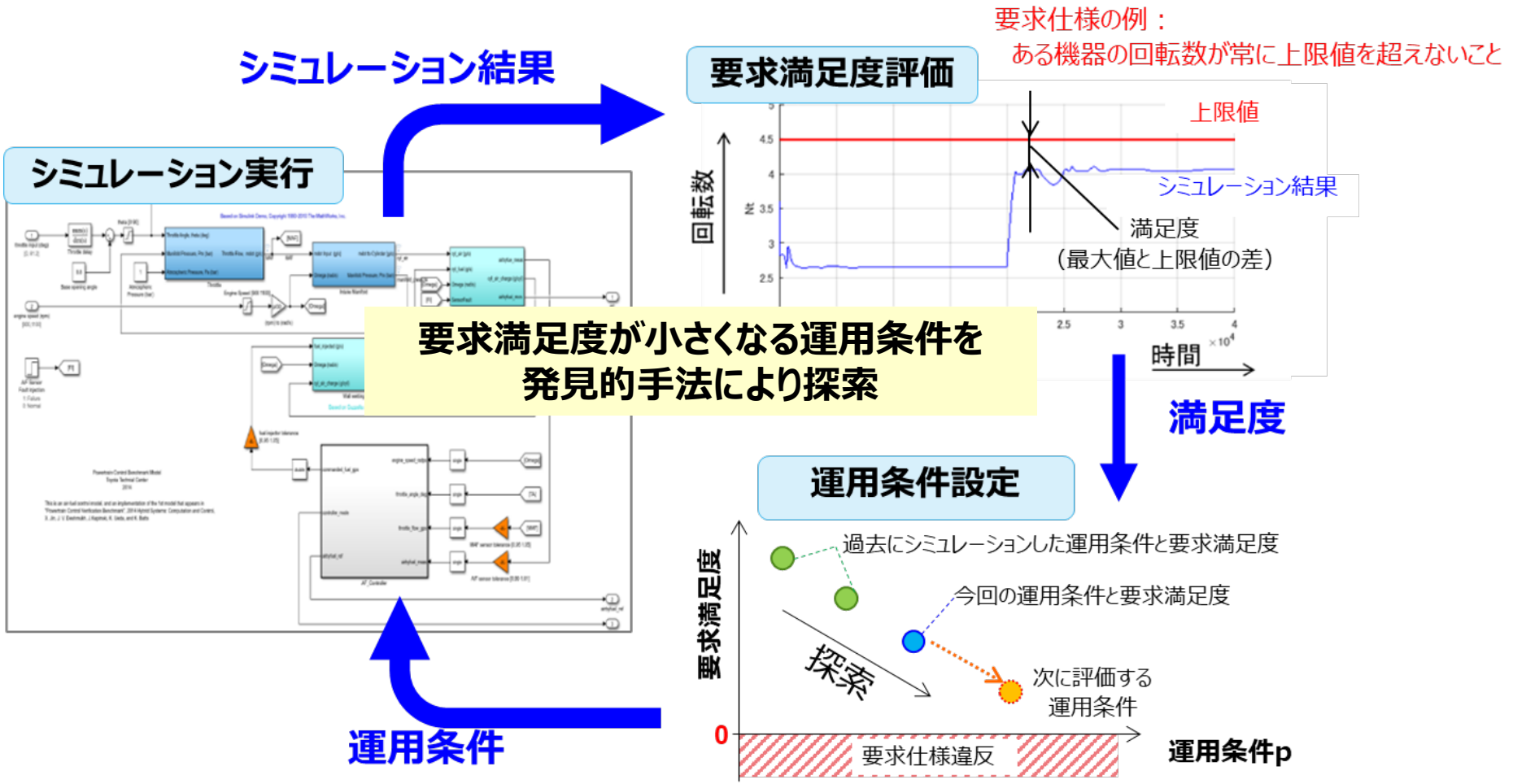
本発表では、複雑な要件/条件を満足させる制御パラメータをFalsificationの技術を用いることにより自動抽出する手法とその結果について説明します。

目次

3. 自動検証技術(Falsification)とは

- シミュレーション結果を要求満足度として評価し、発見的手法(※1)により**要求仕様を違反する運用条件を探索**する技術。

※1　焼きなまし法や山登り法等、評価関数の勾配を用いずに最適解を探索する手法



画像出典元 https://github.com/decyphir/breach/blob/master/Examples/Simulink/AbstractFuelControl/AbstractFuelControl_M1.slx

3. 自動検証技術(Falsification)とは

- 要求満足度を定量評価するため、**要求仕様は論理式で定義**する必要がある。
- 論理式の各作用素(※3)に対応する満足度の評価式が定義されている。

※3 ¬(否定), ∨(論理和), ∧(論理積), →(含意), □(常に真), ◇(いつか真) 等がある。

＜例＞

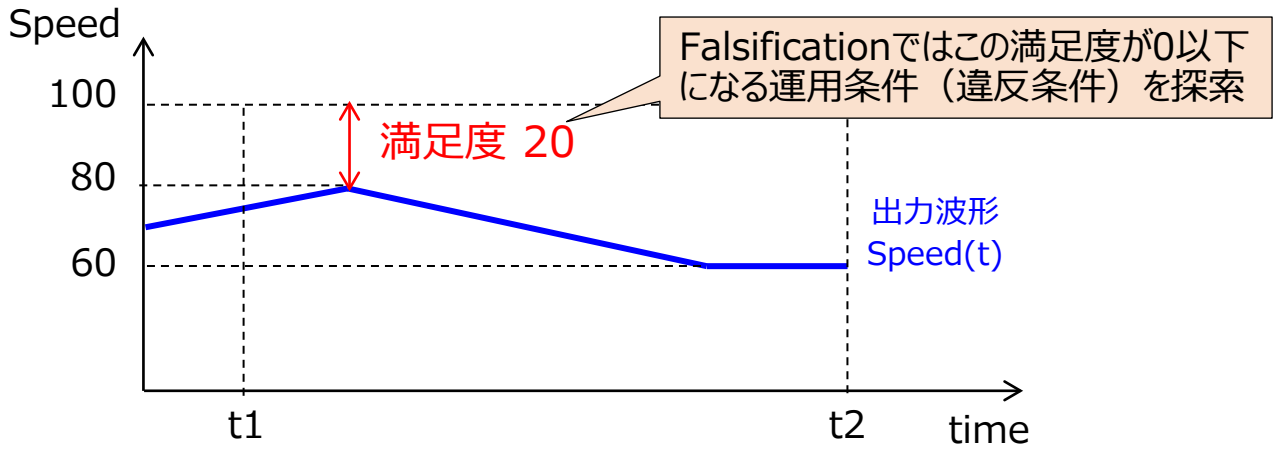
要求仕様： □[t1,t2](Speed ＜100)

シミュレーション結果(出力波形)： Speed(t)

区間 [t1,t2]で**つねに** Speed＜100であること。
つまり、区間[t1,t2]で一瞬でもSpeed≧100であれば要求仕様違反

満足度評価式： min [t1,t2] {100－Speed(t)}
＝20

区間 [t1,t2]における、100－Speed(t)の最小値



Falsificationではこの満足度が0以下になる運用条件（違反条件）を探索

目次

1. 三菱重工のデジタルイノベーションブランドΣSynX

2. V字型開発プロセスと検証技術

3. 自動検証技術 (Falsification)とは

4. Falsificationの応用ー設計パラメータ最適化ー

5. NII様との共同研究成果

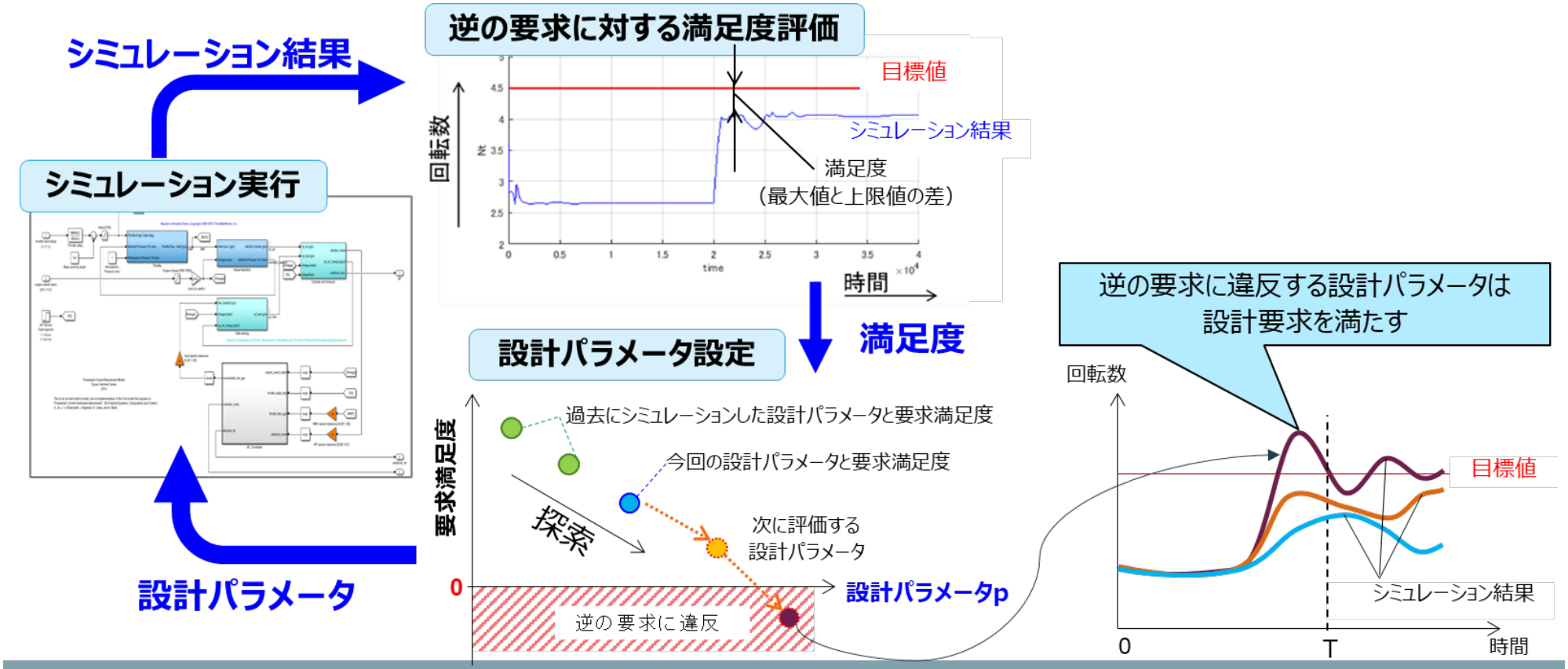
6. まとめ

4. Falsificationの応用　– 設計パラメータ最適化 –

- ”運用条件”を”設計パラメータ”に置き換え、**設計要求と逆の要求を論理式化**し、自動検証を行うことで、設計要求を満たすパラメータを探索する。

設計要求：
ある機器の回転数が**T秒以内に目標値を超える**こと

逆の要求：
ある機器の回転数が**T秒間の間、常に目標値を超えない**こと
□_[0,T] (回転数(t) ＜100)



4. Falsificationの応用　– 設計パラメータ最適化 –

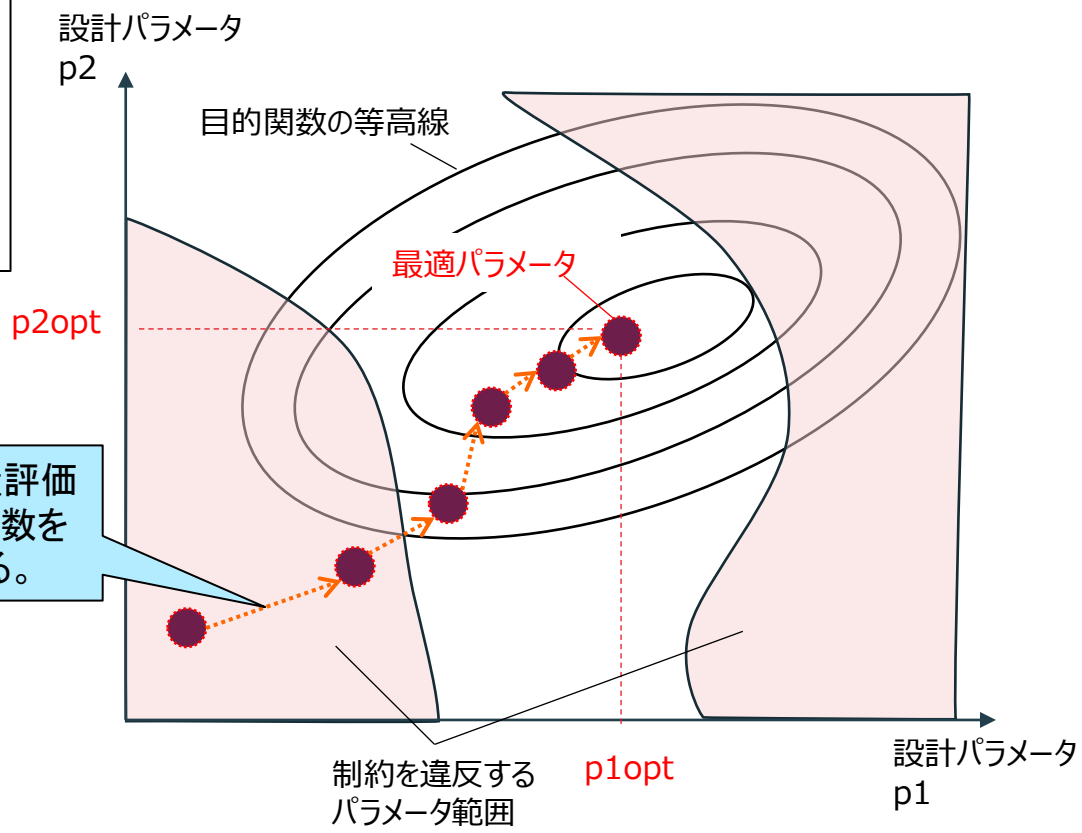
- Falsificationを用いて最適な設計パラメータの探索が可能。
- **時間の概念を含む複雑な制約を扱える**点がポイント。

最小化したい目的関数
　F(x1(p1,p2, t), x2(p1, p2, t))
制約 1
　x1(p1,p2, t)はT1秒以内に目標値X1を超えること
制約 2
　x2(p1,p2, t)はT2秒以上継続して閾値Cを超えないこと

F:目的関数(最大消費電力等)
x1,x2：状態変数(回転数、温度、速度等)
p1,p2：設計パラメータ(制御ゲイン等)
t：時間

目的関数、制約の満足度を定量評価しながら、制約を満足し、目的関数を最小化するパラメータを探索する。

<最適パラメータ探索イメージ>



目次

5. NII様との共同研究成果：あるプラントにおける設計要件

- 大規模プラントの設計問題(数十個の設計パラメータ調整)を対象として選定

制約条件

必須要件 1 ： $H_1 \geq \Theta_4^1$ かつ $H_2 \geq \Theta_3^2$ に一度でも到達すること.

必須要件 2 ： Gの値は常に領域4に入らないこと.

評価関数

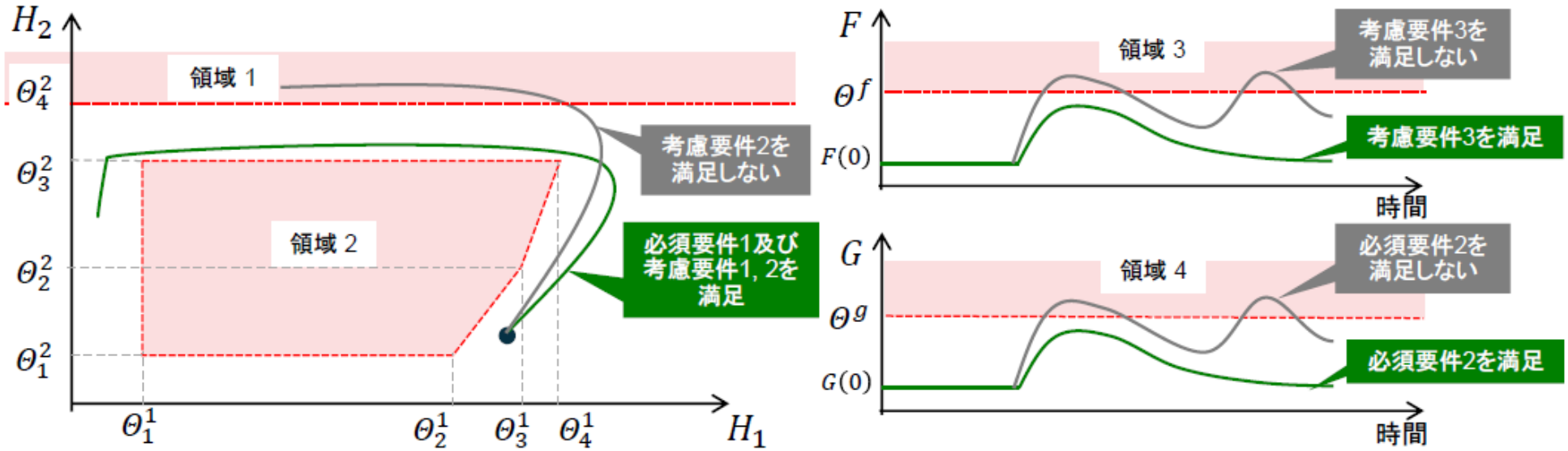
考慮要件 1 ： (H_1, H_2) の値は常に領域2に入らないこと.

考慮要件 2 ： H_2 の値は常に領域1に入らないこと.

考慮要件 3 ： F の値は常に領域3に入らないこと.

※評価時間は60[s]

※F,G,Hは温度、圧力、流量のようなもの



課題①：複数タイプ/スケールの要件を同時に満たすパラメータを探索する必要がある

課題②：”量“と”時間”を両方扱う必要がある※

※つまり”違反量”も”違反時間”も短いほうが望ましい

5. NII様との共同研究成果：課題と打ち手

課題①：複数タイプ/スケールの要件を同時に満たすパラメータを探索する必要がある

MCR（Multiple Constraint Ranking）を用いた制約付き最適解探索

要件　$\varphi^{AT} :\equiv \varphi_1^{AT} \wedge \varphi_2^{AT} \wedge \varphi_3^{AT}$

個々の要件に対する評価値

		φ_1^{AT}（目的関数）	φ_2^{AT}	φ_3^{AT}
個体	u_1	1400	59.9	-3
	u_2	-9	2	1
	u_3	-180	2	-1

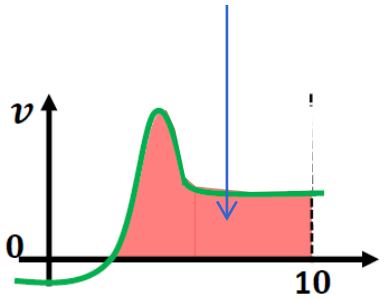
	φ_1^{AT} 評価値	φ_2^{AT} (違反度)	φ_3^{AT} (違反度)	満たさない要件の数	適応度
u_1	1st/ 1400	1st/ 0	3rd/ -3	2nd/ 1	7 (= 1 + 1 + 3 + 2)
u_2	2nd/ -9	1st/ 0	1st/ 0	1st/ 0	5 (= 2 + 1 + 1 + 1)
u_3	3rd/ -180	1st/ 0	2nd/ -1	2nd/ 1	8 (= 3 + 1 + 2 + 1)

課題②：”量“と”時間”を両方扱う必要がある※

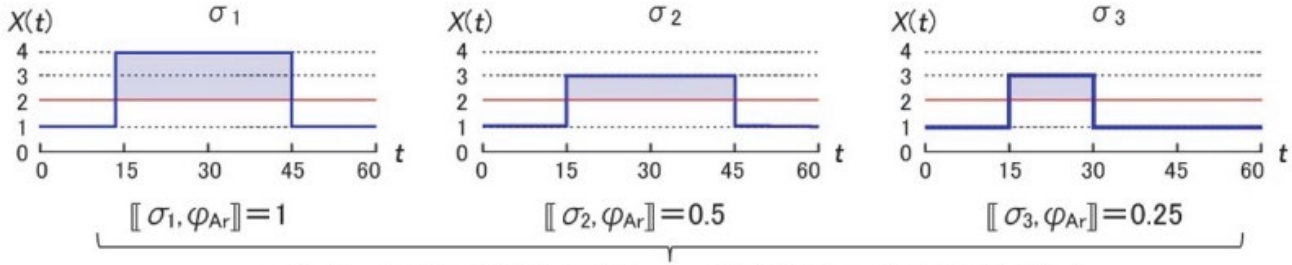
“Area”関数を新たに作成

Area関数

禁止領域に入る量と入っている時間を考慮した余裕度として扱う。



要件：$\varphi_{Ar} \equiv \mathrm{Area}_{[0,60]}(X>2)$



$X(t)$が2を超過する量，超過している時間が短い程評価値が小さい

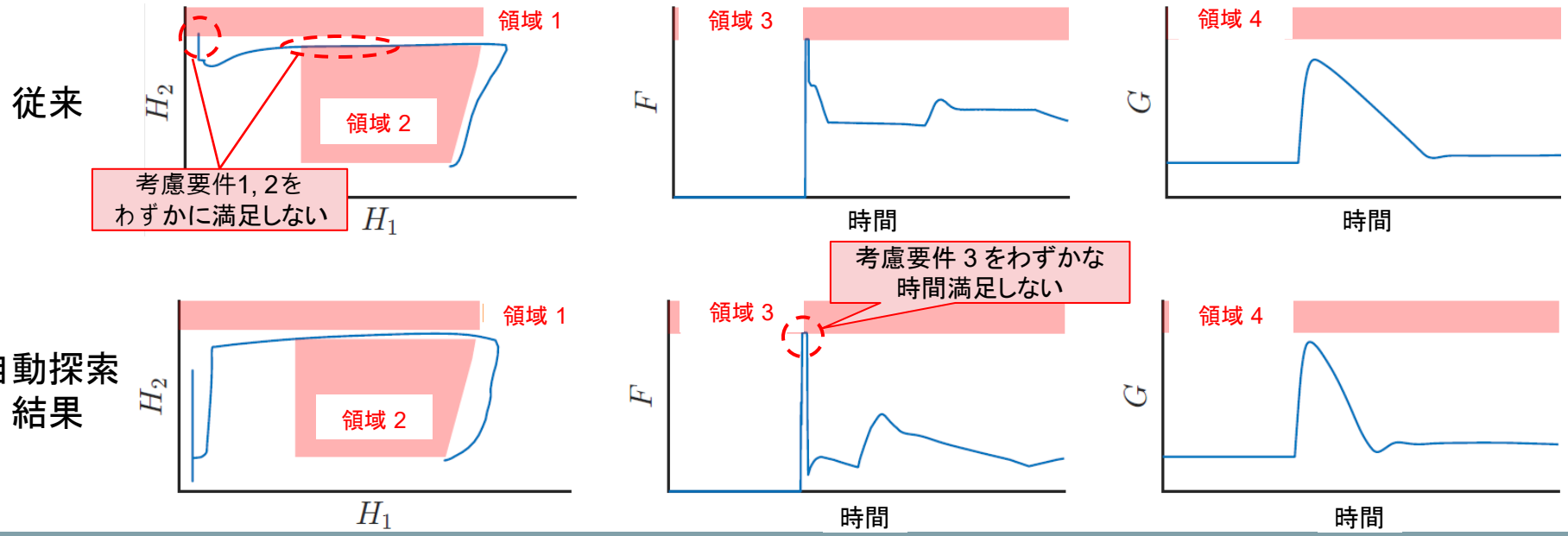
σ：シミュレーション出力

$[\![\sigma, \varphi]\!]$：要件φに対するシミュレーション出力σの評価値

5. NII様との共同研究成果：計算例

- 大規模プラントの設計問題(数十個の設計パラメータ調整)に対して本手法を適用した。
- 熟練者が試行錯誤により設計したパラメータ(従来)，及び３時間（7 000 回以上の探索）の自動探索により得られたパラメータでシミュレーションした結果を下図に示す。
- 自動探索により得られたパラメータは全必須要件を満たし、考慮要件3を僅かに違反するのみであり，熟練者の設計に匹敵する結果が熟練者のノウハウ無しに自動的に得ることができた。

必須要件 1 ： $H_1 \geq \theta_4^1$ かつ $H_2 \geq \theta_3^2$ に一度でも到達すること.
必須要件 2 ： Gの値は常に領域4に入らないこと.
考慮要件 1 ： (H_1, H_2) の値は常に領域2に入らないこと.
考慮要件 2 ： H_2 の値は常に領域1に入らないこと.
考慮要件 3 ： F の値は常に領域3に入らないこと.



目次

6. まとめ

目的	**複雑な要求仕様を満足させる設計パラメータの自動設計**
課題	• ①“複雑な要求仕様”を**正確に**評価関数で表現した上でパラメータ探索するのが困難 • 従来の自動検証技術を応用したパラメータ探索技術の課題は以下。 ② **スケール/タイプの違う複数の要件**を満たす設計パラメータを探索が困難である。 ③ “しきい値を超える量も時間も短い方がよい”というように**違反量と違反時間の両方**に関する要件を扱うことができない。
解決策	□ [①] **信号時相論理**(STL)で仕様を表現し、**Falsification技術**によりパラメータ探索。 □ [②] **MCR（Multiple Constraint Ranking）を用いた制約付き最適解探索**により複数要件間のスケール問題を解消。 □ [③] 信号時相論理を拡張させる(**“Area関数”を導入する**)ことで、“量”と”時間”を含む複雑な要求仕様を表現
効果	大規模かつ複雑なプラントに対して、複数要件仕様を満たすよう数十個の制御パラメータを調整する対象に対して、以下の効果を得た。 ➢ 調整時間の短縮：7日以上(従来) →**3時間以下** ➢ 品質の改善：考慮要件※1を満たさない場合が多い →**ほぼ全ての要件を満たす**。 ※1: 考慮要件:必須ではないが、”できれば”満たした方が良い要件。

MOVE THE WORLD FORWARD

MITSUBISHI
HEAVY
INDUSTRIES
GROUP