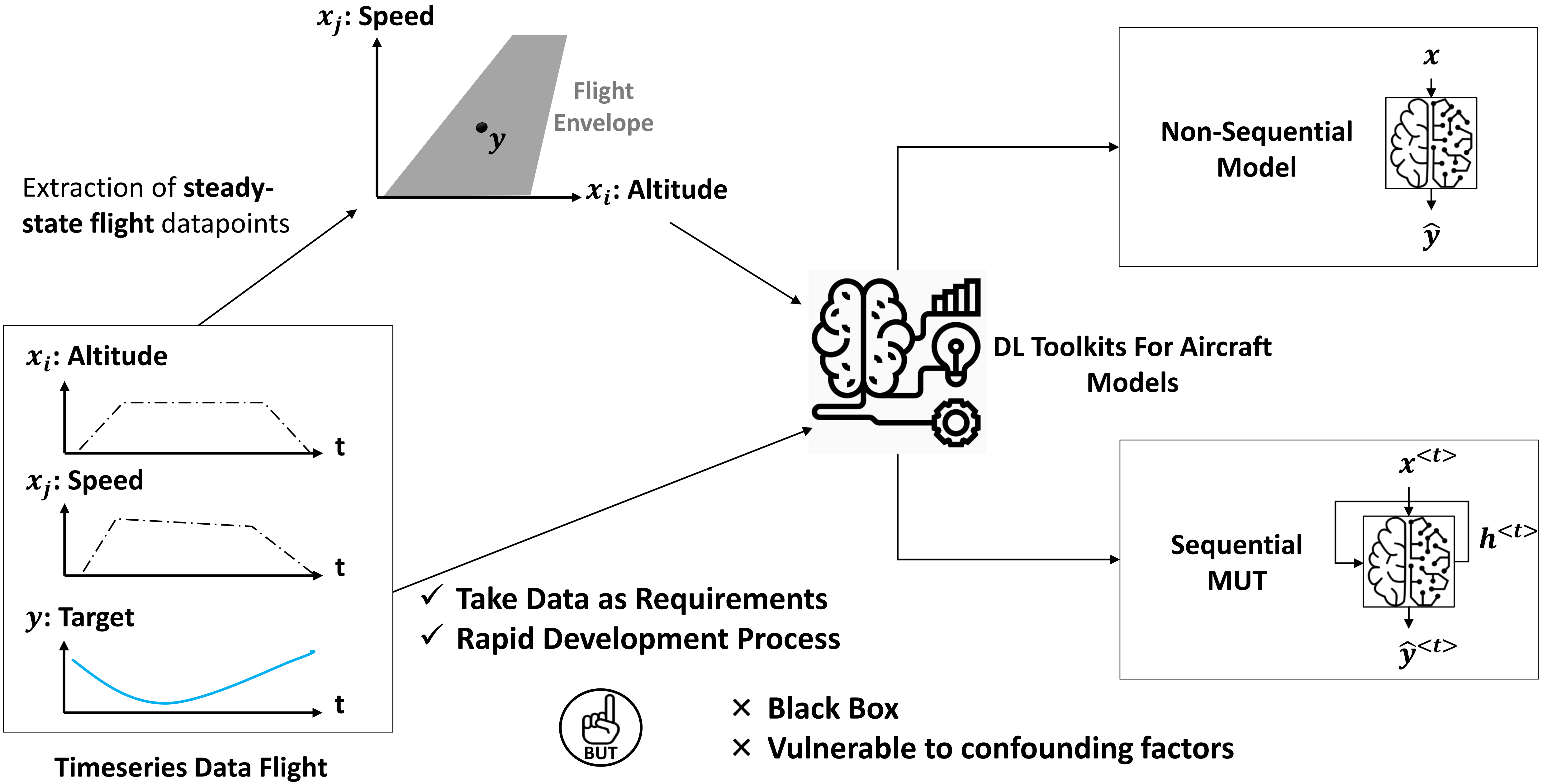
Ingenuity
in Flight.

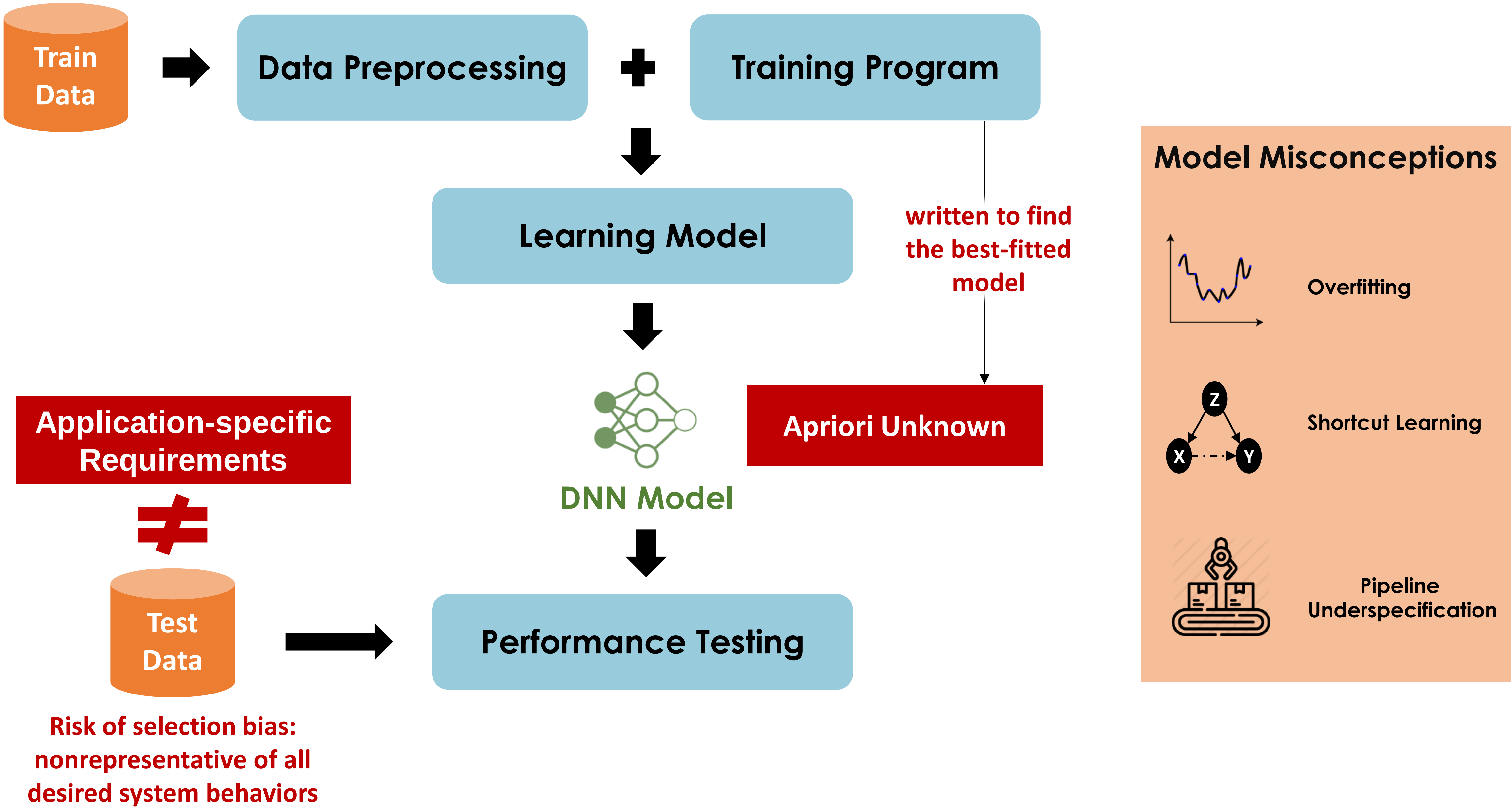
Domain-Aware Deep Learning Testing for Aircraft Models

Houssem Ben Braiek, Ph.D. DEEL/Bombardier

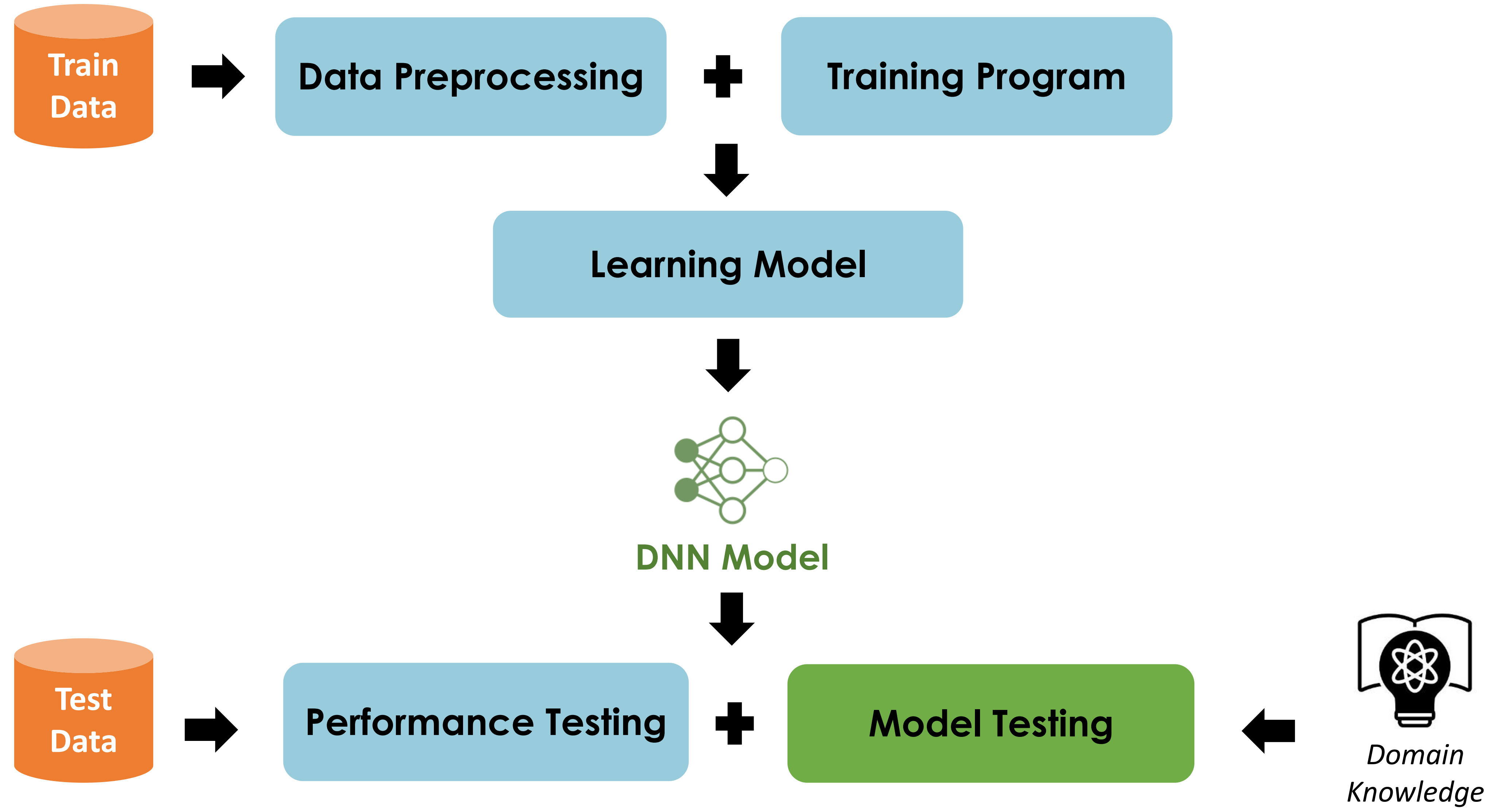
DL-based A/C System Performance Models



Challenges of Quality Assurance for DL Models



Need for Domain-Aware DL Testing Models



Goal of Domain-Aware DL Testing Models

Tradeoff

Statistical Testing

Estimate the **iid performance** of the model for completely **new inputs**.

$$\boldsymbol{Err} = \sum_{i \in \boldsymbol{D}_{test}} \left(\hat{\boldsymbol{y}}^{(i)} - \boldsymbol{y}^{(i)}\right)^2$$

Use unseen test data $\boldsymbol{D}_{test}$ as a proxy for future entries ($\boldsymbol{x}_{new}$).

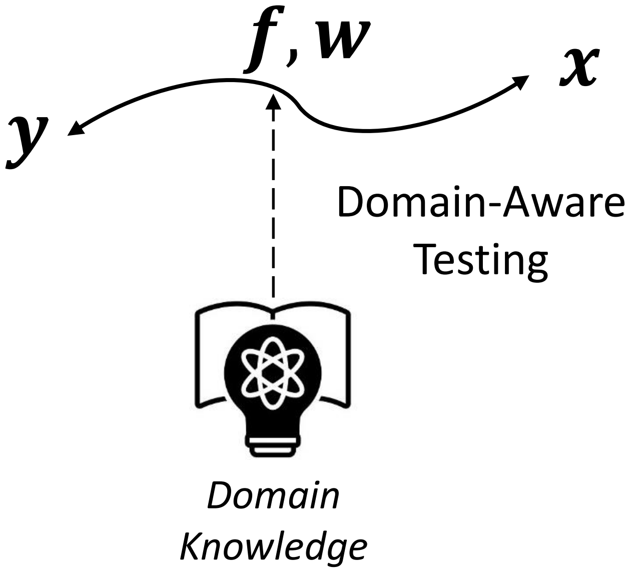
$$\boldsymbol{D}_{test} = \left\{\left(\boldsymbol{x}^{(i)}, \boldsymbol{y}^{(i)}\right)\right\}_{\mathrm{i} \in [1,\mathrm{N}]}$$

Collection of $\boldsymbol{D}_{test}$ is costly in aircraft industry

Model Testing

Test the **internal logic/mappings** of the model against the prior knowledge on the nature of the relation between $\boldsymbol{x}$ and $\boldsymbol{y}$.

Unknown $\boldsymbol{f}^*$? $\boldsymbol{w}^*$?



Goal of Domain-Aware DL Testing Models

From Deep Learning Perspective:

Best-fitted DL solution simulates perfectly the designed system behavior under similar or close operating conditions.

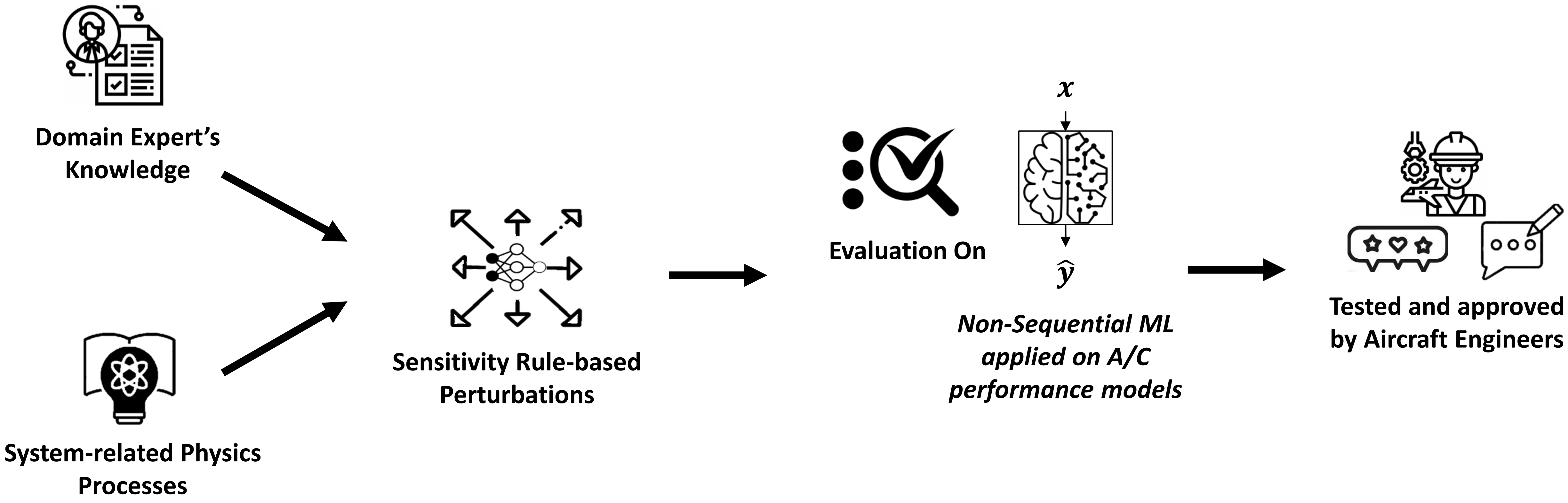
From Engineering Perspective:

A/C performance models should simulate accurately the designed system behavior given any foreseeable operating conditions.

Domain-aware Testing Approaches contribute to close this gap and to steer the DL model development towards solving the real target problem.

Physics-guided Adversarial Machine Learning

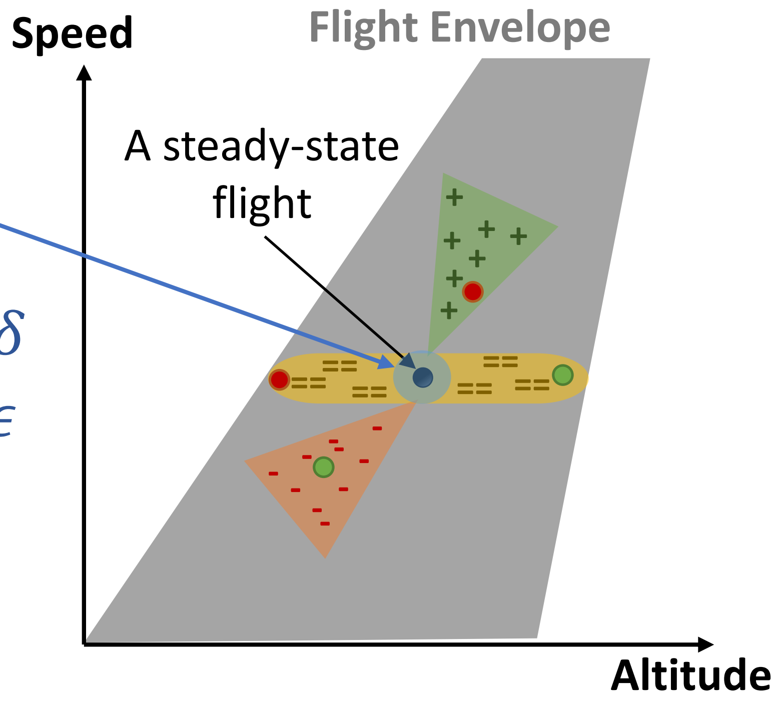
Definition of Physics-grounded Sensitivity Rules



Novelty of Physics-guided Adversarial ML

δ-local adversarial robustness

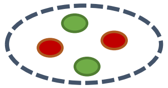
$$\forall\, x' \colon \|x - x'\|_p \leq \delta$$
$$\Rightarrow f(x) - f(x') \leq \epsilon$$



Relying on Physics-grounded Sensitivity rules :

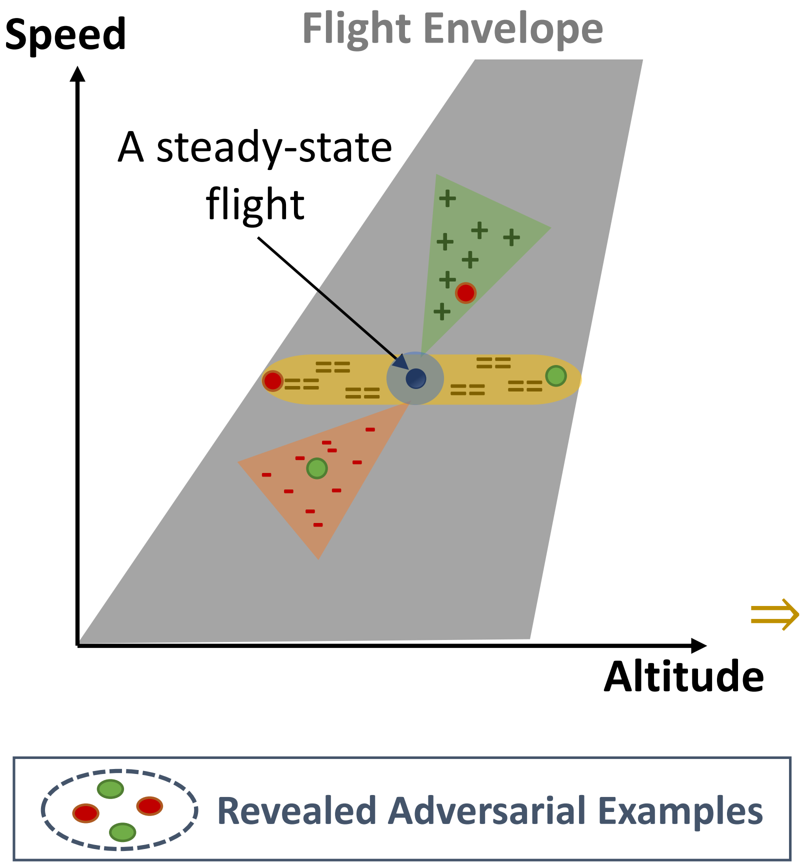
We perform invariance/directional expectation tests.

1. **For which the prediction should almost hold**
2. **For which the prediction should increase**
3. **For which the prediction should decrease**



These represent the revealed adversarial inputs x for which the predictions are not consistent with the foreknown local sensitivities.

Types of Physics-based Adversarial Test/Fix



Physics-based Invariance Test/Fix (Steadying)

1. For which the prediction should almost hold

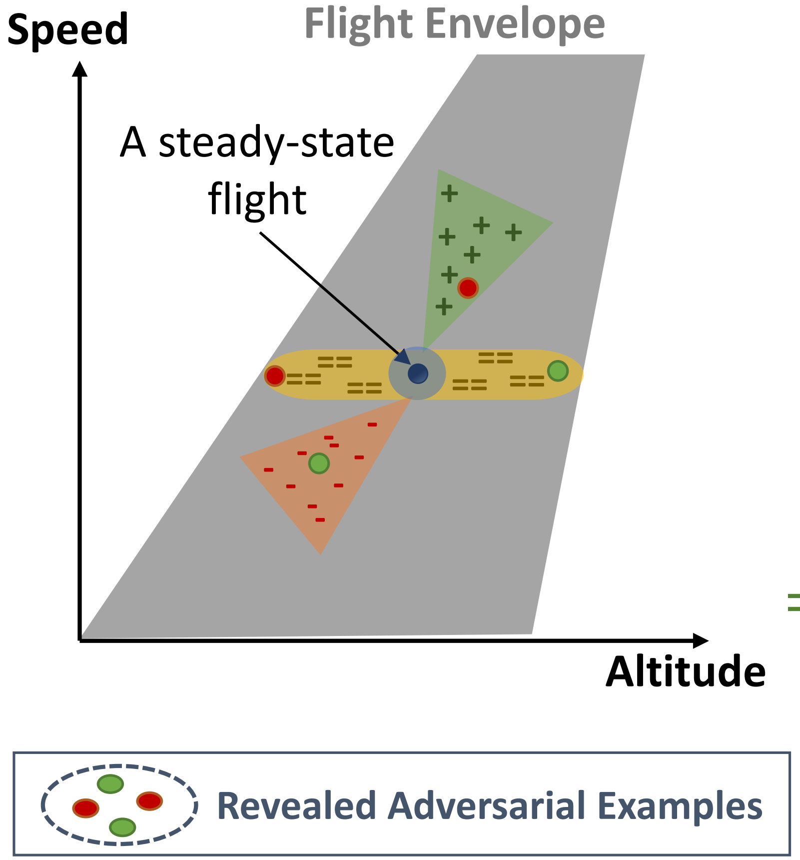
$$x_i \nearrow, x_{i+1} \searrow, \dots, x_n \leftrightarrow \Rightarrow f \leftrightarrow$$ [Rule Spec]

$$\forall\, x', \forall i \in I_{pr}: (x_i - x_i') \leq \delta_i$$ [Input Perturbation]

$$\Rightarrow |f(x) - f(x')| \leq \epsilon$$ [Test Assertion]

$$\Rightarrow R(x, x') = \max\left(tol^2, \left(f(x) - f(x')\right)^2\right) - tol^2$$ [Regularization Term]

Types of Physics-based Adversarial Test/Fix



Physics-based Directional Expectation Test/Fix (Increasing)

2. For which the prediction should increase

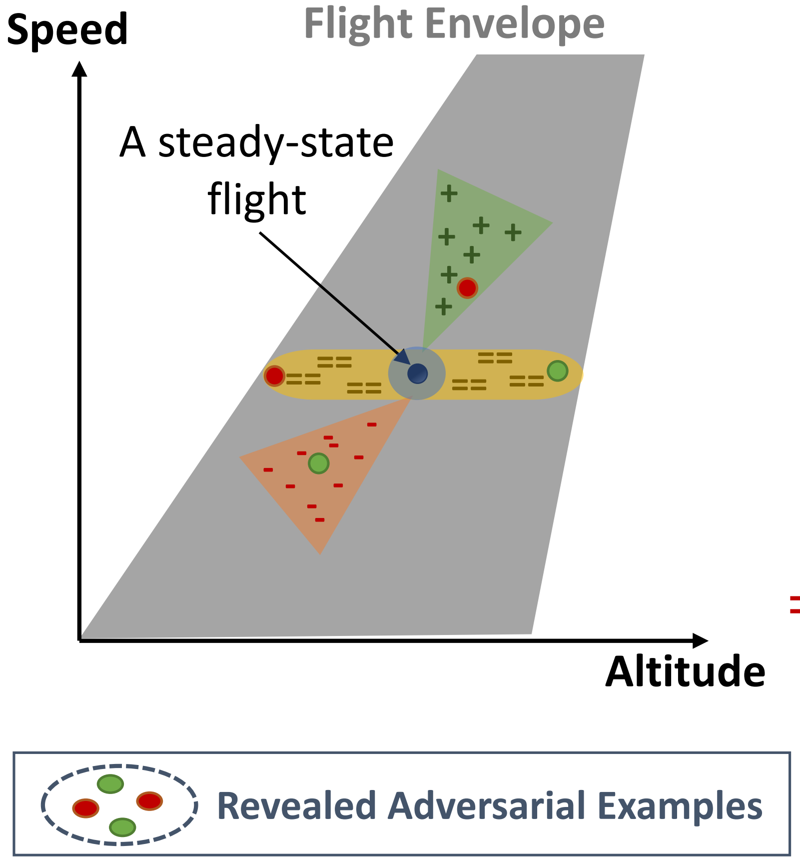
$$x_i \nearrow, x_{i+1} \searrow, \ldots, x_n \leftrightarrow \; \Rightarrow f \nearrow$$ [Rule Spec]

$$\forall\, x', \forall i \in I_{inc}, (x_i - x_i') \leq \delta_i$$ [Signed Input Perturbation]

$$\Rightarrow f(x) \geq f(x')$$ [Test Assertion]

$$\Rightarrow R(x, x') = (\max(tol, f(x) - f(x')) - tol)^2$$ [Regularization Term]

Types of Physics-based Adversarial Test/Fix



Physics-based Directional Expectation Test/Fix (Decreasing)

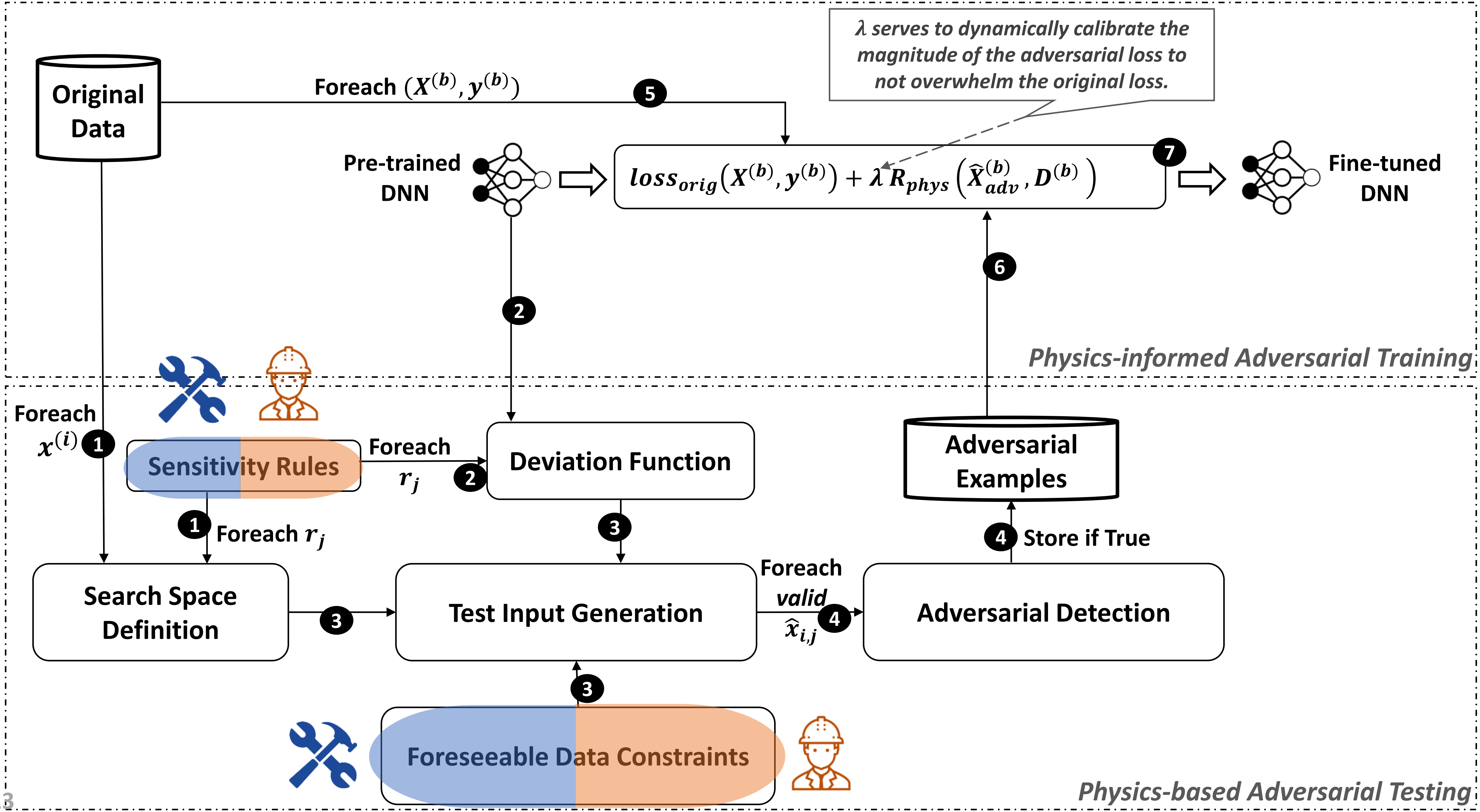
3. For which the prediction should decrease

$$x_i \nearrow, x_{i+1} \searrow, \ldots, x_n \leftrightarrow \; \Rightarrow f \searrow$$ [Rule Spec]

$$\forall\, x', \forall i \in I_{dec} : (x_i - x_i') \le \delta_i$$ [Signed Input Perturbation]

$$\Rightarrow f(x) \le f(x')$$ [Test Assertion]

$$\Rightarrow R(x, x') = (\max(tol, f(x') - f(x)) - tol)^2$$ [Regularization Term]

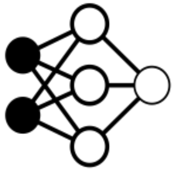


λ serves to dynamically calibrate the magnitude of the adversarial loss to not overwhelm the original loss.
Original Data
Foreach $(X^{(b)}, y^{(b)})$
5
Pre-trained DNN
$loss_{orig}(X^{(b)}, y^{(b)}) + \lambda R_{phys}(\hat{X}^{(b)}_{adv}, D^{(b)})$
7
Fine-tuned DNN
6
2
Physics-informed Adversarial Training
Foreach $x^{(i)}$
1
Sensitivity Rules
Foreach r_j
2
Deviation Function
Adversarial Examples
1
Foreach r_j
3
4
Store if True
Search Space Definition
3
Test Input Generation
Foreach valid $\hat{x}_{i,j}$
4
Adversarial Detection
3
Foreseeable Data Constraints
Physics-based Adversarial Testing

Study Cases for Empirical Evaluation

Datasets

Base Model



Feedforward Neural Networks

Model	Predicted Target	Description
A/C Perf	α: angle of attack	The model maps steady-state angle of attack (α) to features related to flight conditions and wing configurations.
WAI. Perf	T_{skin}^{b}: A-wing leading-edge skin temperature T_{skin}^{b}: B-wing leading-edge skin temperature	The model maps the states of skin temperature sensors to features related to flight conditions, wing configurations, and high-pressure pneumatic system conditions at the wing root.

Some Results of the Empirical Evaluation

Comparison between #adversarials Before and After fine-tuning

SYS	G	pre-fixed	post-fixed	Improv.(%)
A-C Perf.	Random	5267	1012	80.78%
	PSO	39551	5747	85.46%
	GA	2850	636	77.68%
WAI Perf.	Random	509	0	100%
	PSO	20545	18	99.91%
	GA	459	4	99.12%

Comparison between unscaled RMSE Before and After fine-tuning

SYS	Target	pre-fixed	Algo	post-fixed
A-C Perf.	α	0.498°	Random	0.497°
			PSO	0.996°
			GA	0.444°
WAI Perf.	T^a_{skin}	4.088°C	Random	4.729°C
			PSO	4.422°C
			GA	3.979°C
	T^b_{skin}	7.524°C	Random	7.921°C
			PSO	6.826°C
			GA	7.163°C

Physics-guided Adversarial Machine Learning

Physics-based Differential DL Testing

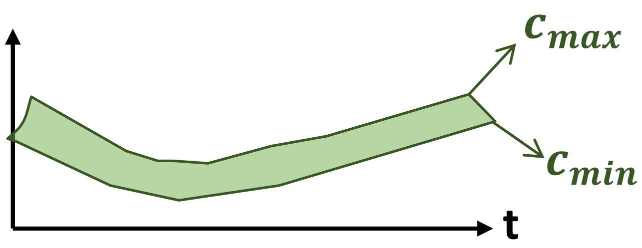
Definition of Physics-based Margin Forecast

Domain Expert's Knowledge

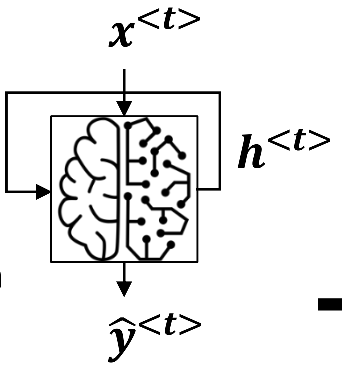
System-related Physics Processes

Bayesian Calibrated Physics Model

To forecast the expected tendency as an evolving margin over time



Evaluation On



Sequential ML applied on A/C performance models

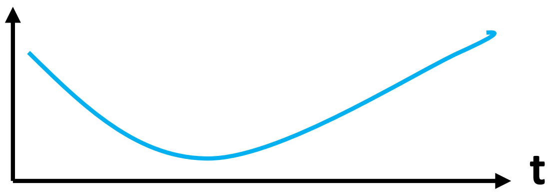
Tested and approved by Aircraft Engineers

Design Both Types of Models

A Train a Sequential ML Model:

$$\boldsymbol{f_{DL}}\ (\boldsymbol{x};\boldsymbol{\theta}) = \boldsymbol{\hat{y}_{DL}}$$

$\boldsymbol{\hat{y}}$: DL Predictions

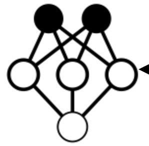


$\boldsymbol{f_{DL}}\ (\boldsymbol{x};\boldsymbol{\theta})$: Universal Approximation Function

$\boldsymbol{\theta}$: Weights & Biases

Data-driven Statistical Learning

Inputs $\boldsymbol{x}$



predicted outputs $\boldsymbol{\hat{y}_{DL}}$

Distance

actual outputs $\boldsymbol{y}$

Loss Estimation

Update Parameters $\boldsymbol{\theta}$ to minimize the loss

B Calibrate a PHYS Model: $\boldsymbol{f_{PHYS}}\ (\boldsymbol{x};\boldsymbol{\theta}) = \boldsymbol{\hat{y}_{phys}}$

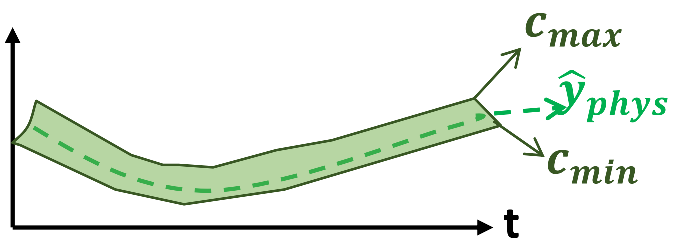
Estimate then:

i) Parameters Uncertainty

ii) Structural Uncertainty

iii) Experimental Uncertainty

$[\boldsymbol{c_{min}}, \boldsymbol{c_{max}}]$: PHYS Conf Intl



$\boldsymbol{f_{PHYS}}\ (\boldsymbol{x};\boldsymbol{\theta})$: Parametric Solution for Differential Equations

$\boldsymbol{\theta}$: Defined Quantities & Coefficients

Bayesian Inference for Model Calibration

$$p(\theta|\hat{y}_{phys}, X) \propto p(\hat{y}_{phys}|\theta, X) \times p(\theta|X)$$

Posterior Probability — Data Likelihood — Prior Probability

i) Parameters Uncertainty ➔ $\forall\alpha \in \theta,\ \ \alpha \sim \mathcal{N}(\mu_\alpha,\ \sigma_\alpha)$

ii) Structural Uncertainty ➔ $y_{actual} \sim \mathcal{N}(\hat{y}_{phys},\ \sigma_y)$

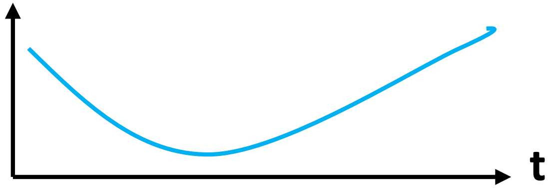
iii) Experimental Uncertainty ➔ $y_{true} \sim \mathcal{N}(y_{actual},\ \varepsilon_{noise})$

Physics-based Differential DL Testing

A **Train a Sequential ML Model:**

$$f_{DL}(x) = \hat{y}_{DL}$$

$\hat{y}$: **DL Predictions**



B **Calibrate a PHYS Model:** $f_{PHYS}(x) = \hat{y}_{phys}$

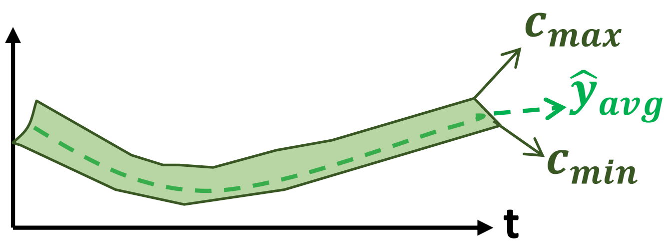
Estimate then:

i) Parameters Uncertainty

ii) Structural Uncertainty

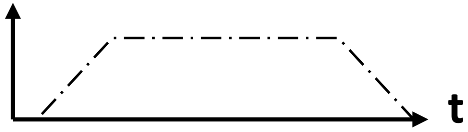
iii) Experimental Uncertainty

$[c_{min}, c_{max}]$: **PHYS Conf Intl**

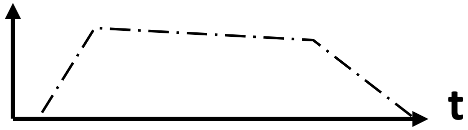


C

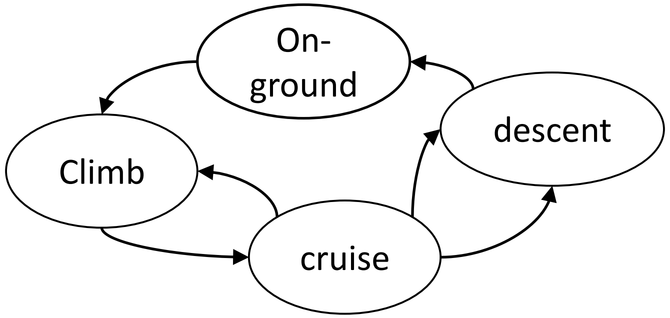
x_i: **Altitude**



x_j: **Speed**



Markovian Stochastic Process for Flight Generator



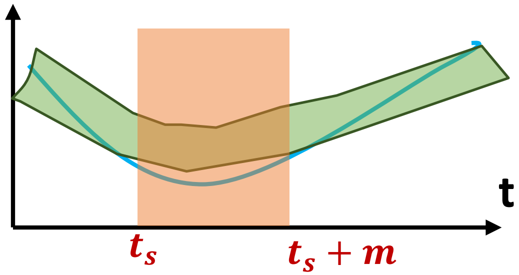
Fit Stochastic Generative Model for Feature Data Distribution

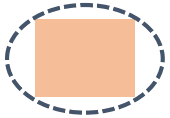
$$P(x_i, x_j)$$

D **Assert that DL predictions are within the PHYS confidence intervals:**

$$\forall x, f_{DL}(x) = \hat{y}_{DL} \notin [c_{min}, c_{max}]$$

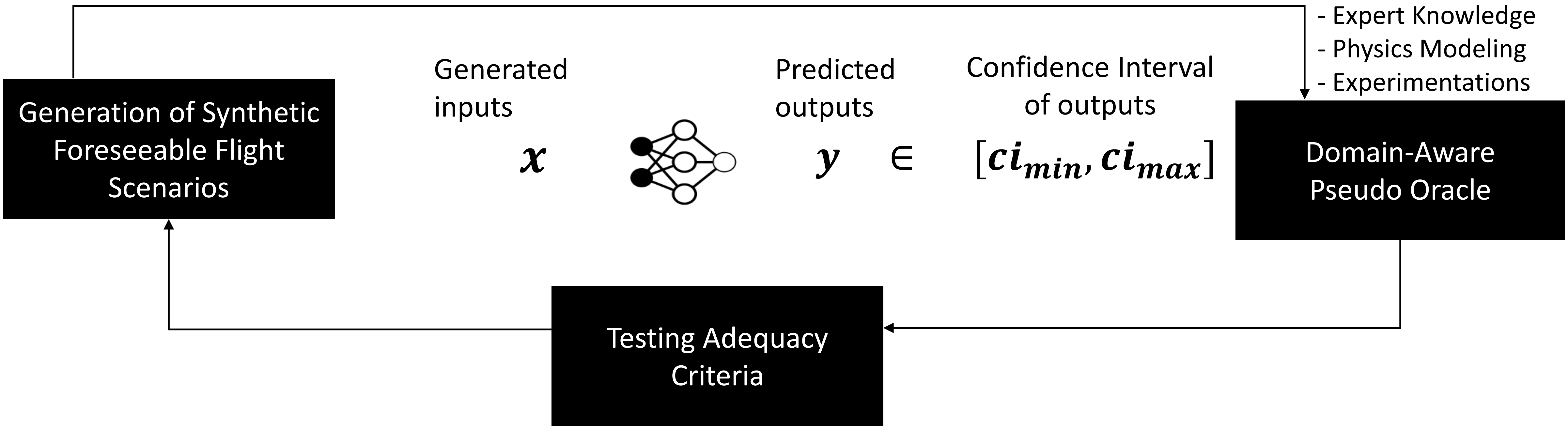
$[x^{<t_s>}, x^{<t_s+m>}]$: **Adversarial Region**



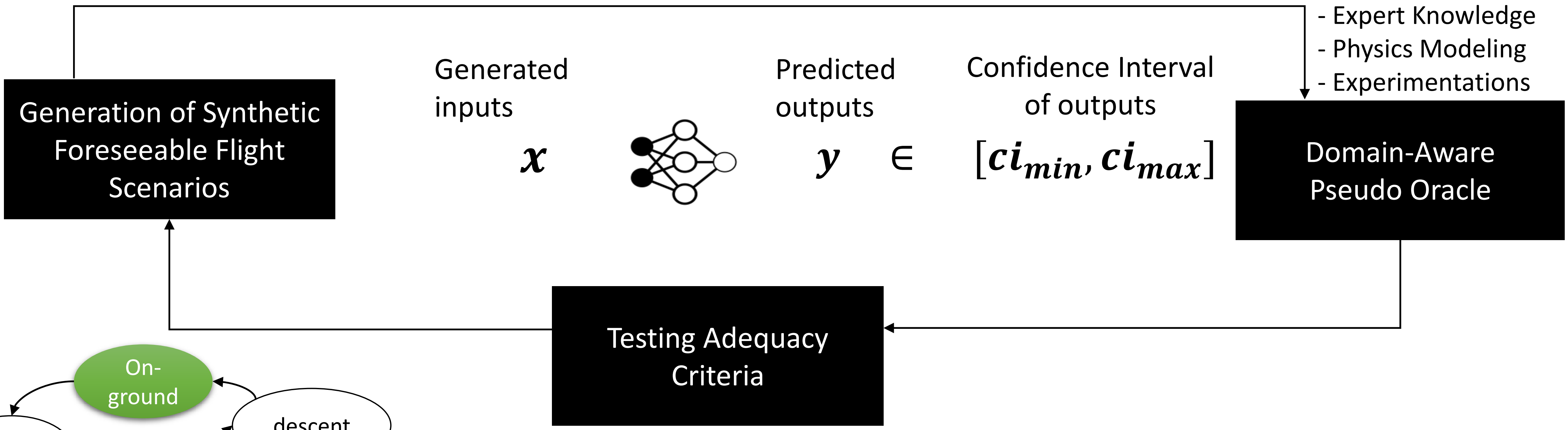


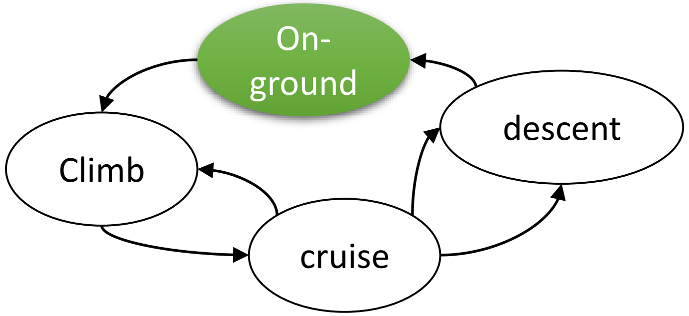
It represents the adversarial input regions for which the predictions are not consistent with the physics-based model.

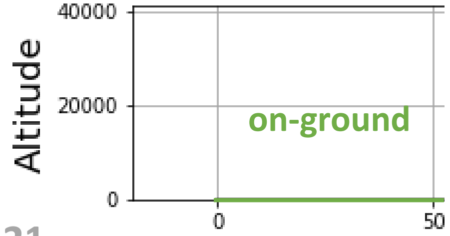
Physics-based Differential Test: Workflow



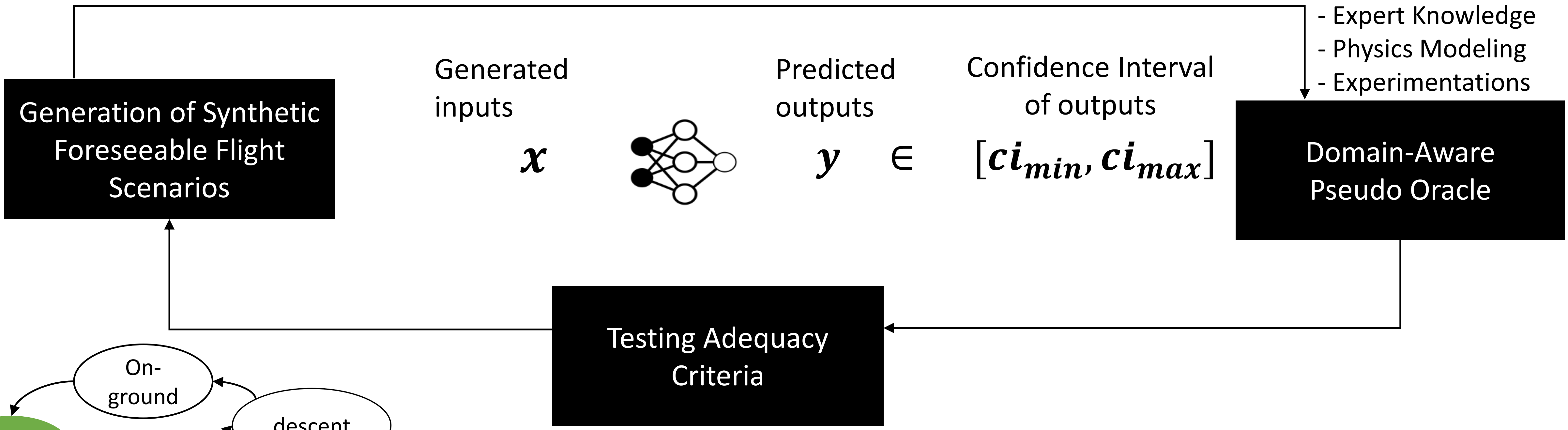
Physics-based Differential Test: Data Generation

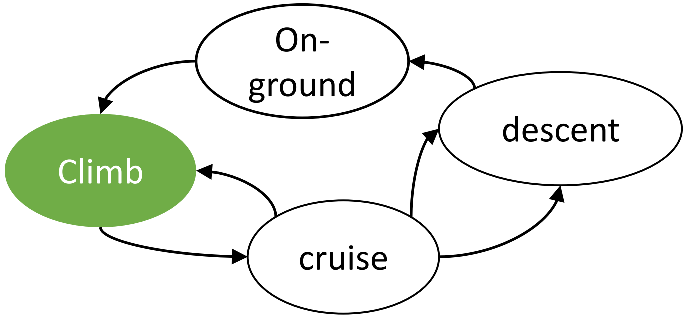


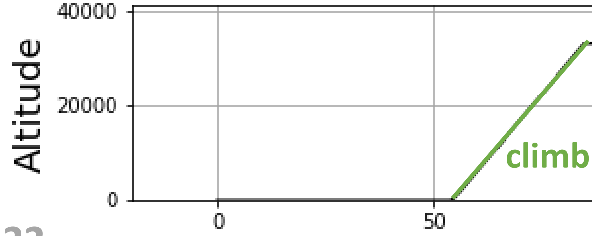




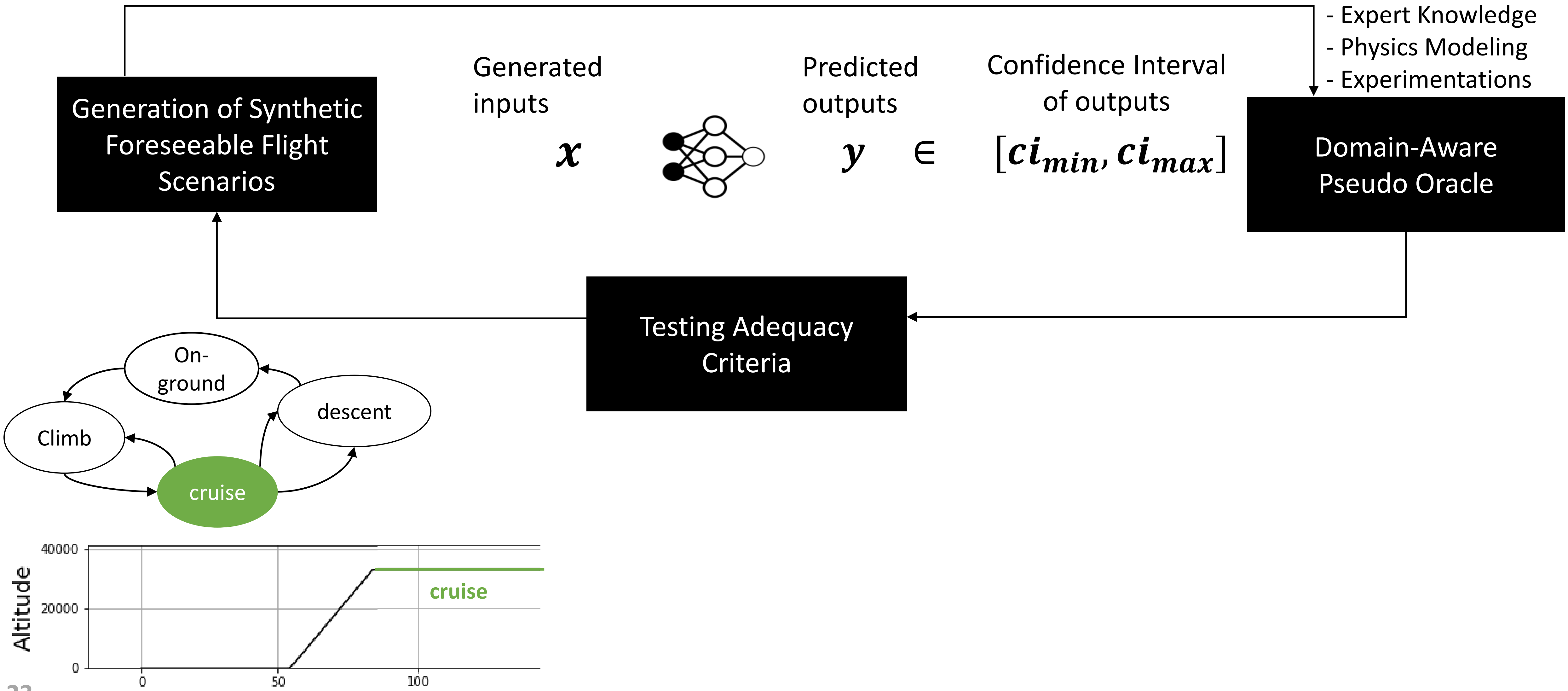
Physics-based Differential Test: Data Generation







Physics-based Differential Test: Data Generation



Physics-based Differential Test: Data Generation

Generation of Synthetic Foreseeable Flight Scenarios

Generated inputs $\boldsymbol{x}$

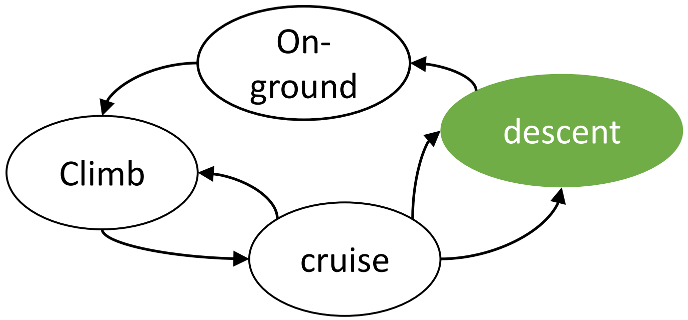
Predicted outputs $\boldsymbol{y} \in [\boldsymbol{ci}_{min}, \boldsymbol{ci}_{max}]$

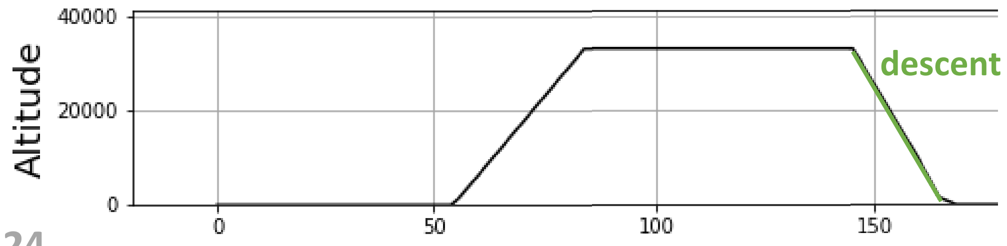
Confidence Interval of outputs

- Expert Knowledge
- Physics Modeling
- Experimentations

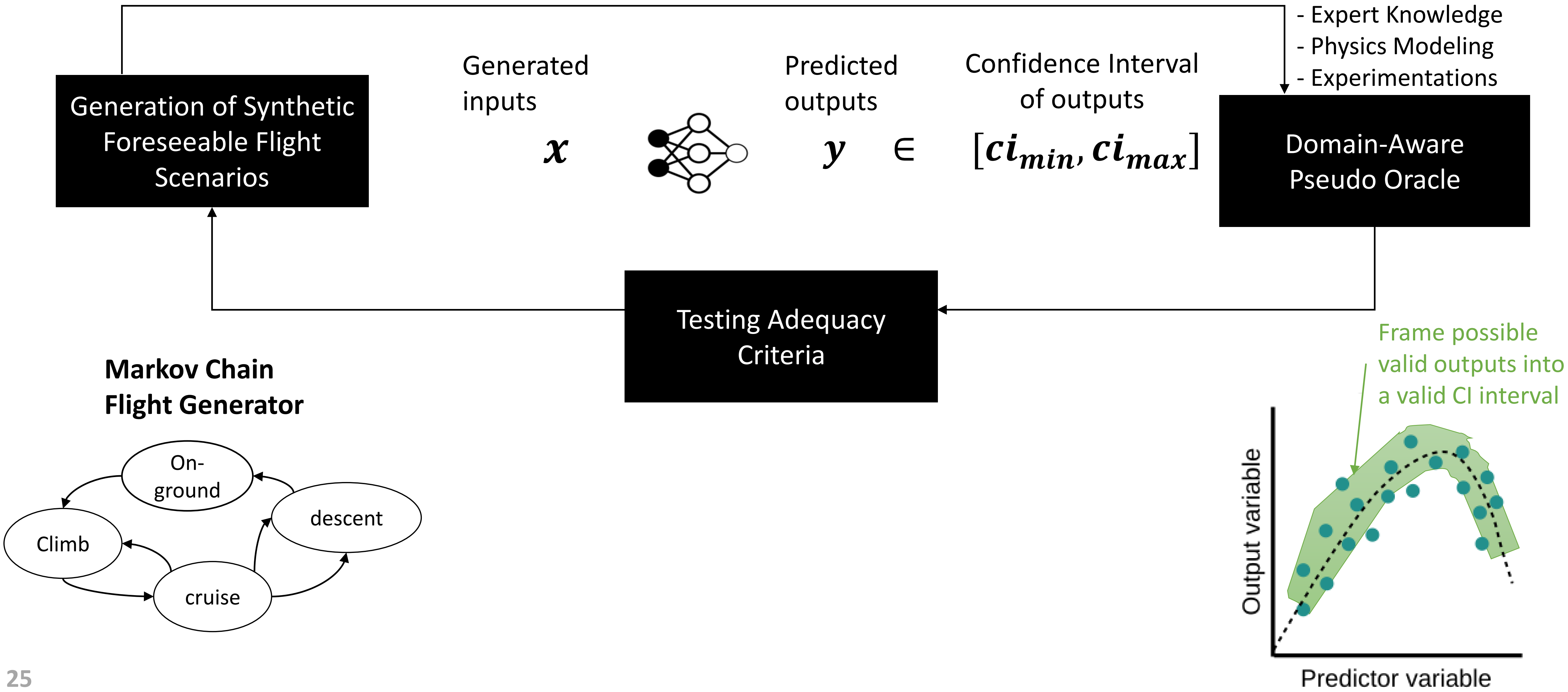
Domain-Aware Pseudo Oracle

Testing Adequacy Criteria





Physics-based Differential Test: Assertions



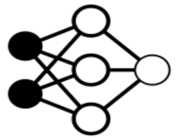
Physics-based Differential Test: Assertions

- Expert Knowledge
- Physics Modeling
- Experimentations

Generation of Synthetic Foreseeable Flight Scenarios

Generated inputs

$\boldsymbol{x}$



Predicted outputs

$\boldsymbol{y} \in$

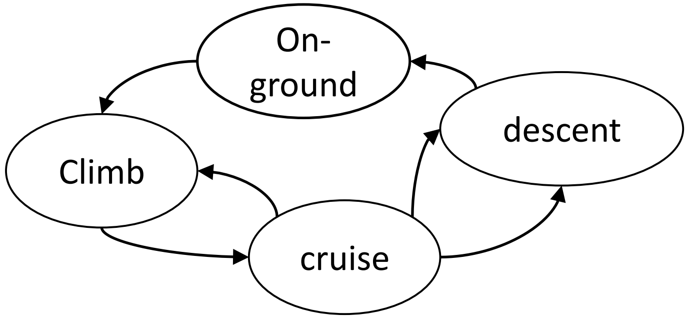
Confidence Interval of outputs

$[\boldsymbol{ci}_{min}, \boldsymbol{ci}_{max}]$

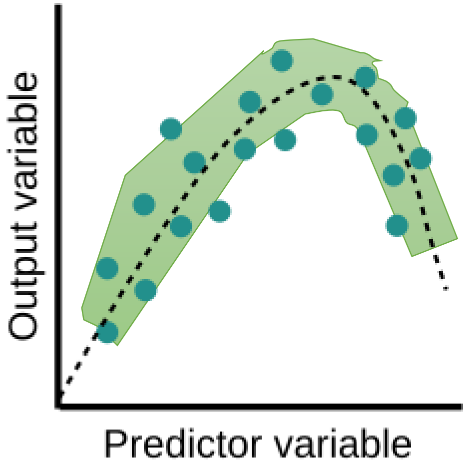
Domain-Aware Pseudo Oracle

Testing Adequacy Criteria

Markov Chain Flight Generator



Bayesian Calibrated Physics-Based Model



Physics-based Differential Test: Improvement

Generation of Synthetic Foreseeable Flight Scenarios

Generated inputs

$\boldsymbol{x}$

Predicted outputs

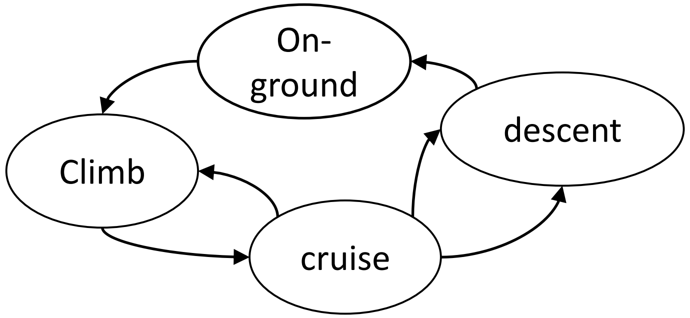
$\boldsymbol{y} \in [\boldsymbol{ci}_{\boldsymbol{min}}, \boldsymbol{ci}_{\boldsymbol{max}}]$

Confidence Interval of outputs

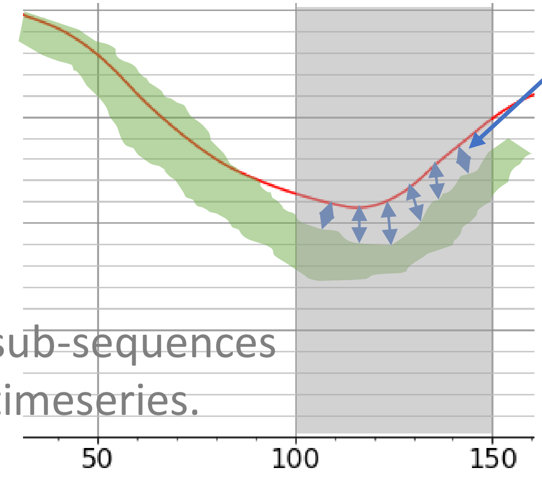
Domain-Aware Pseudo Oracle

Testing Adequacy Criteria

Markov Chain Flight Generator



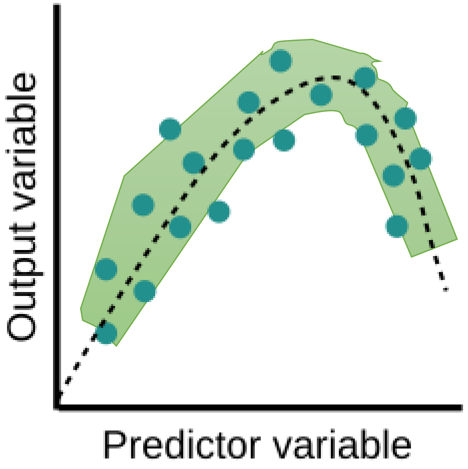
Fine-grained Measure of the Output Deviation

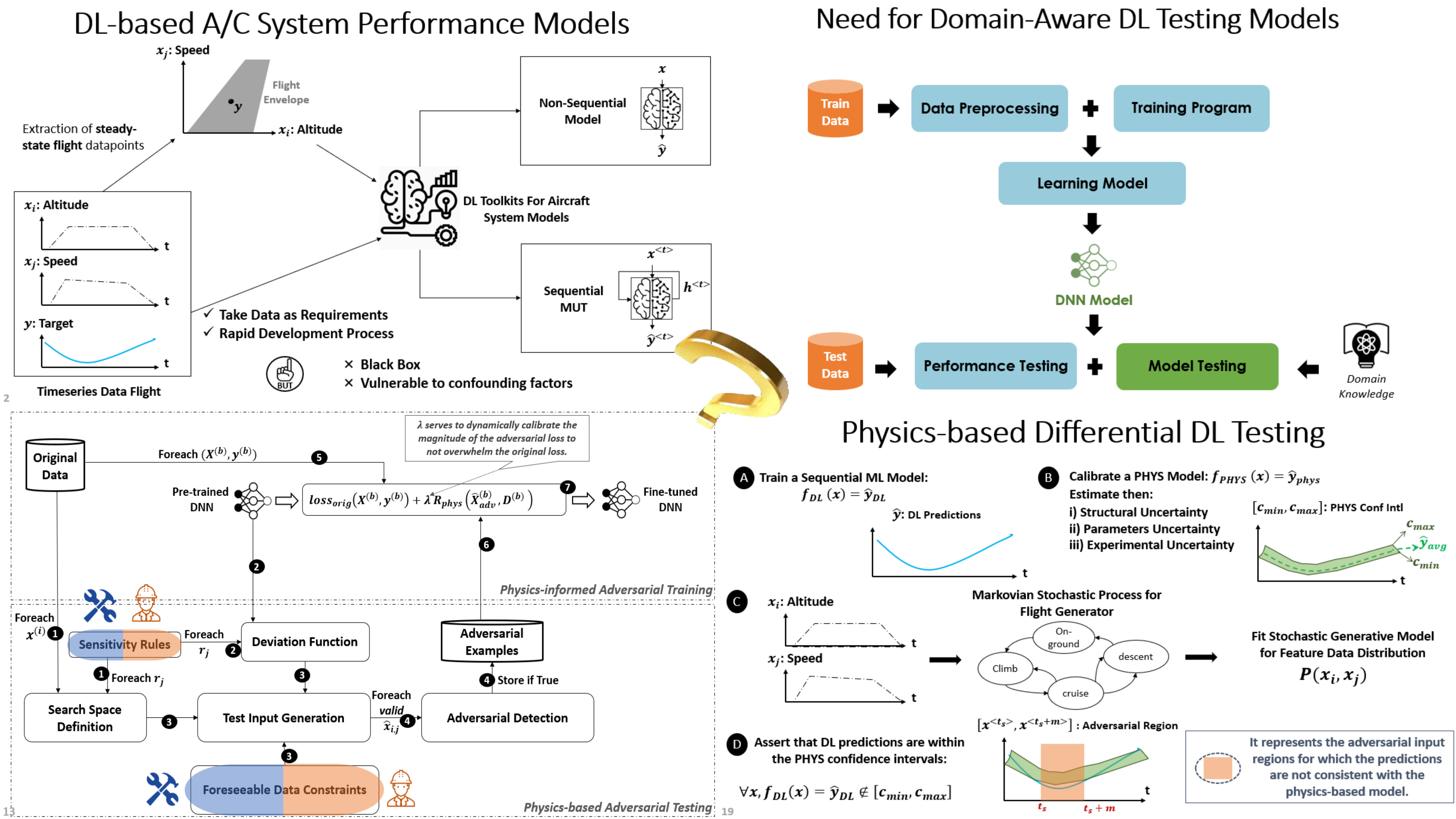


Compute the distances between predictions and expected valid ranges.

Extract faulty sub-sequences of forecasted timeseries.

Bayesian Calibrated Physics-Based Model





DL-based A/C System Performance Models
x_j: Speed
Flight Envelope
y
x_i: Altitude
Extraction of **steady-state flight** datapoints
x_i: Altitude
x_j: Speed
y: Target
t
Timeseries Data Flight
Non-Sequential Model
x
$\hat{y}$
DL Toolkits For Aircraft System Models
Sequential MUT
$x^{<t>}$
$h^{<t>}$
$\hat{y}^{<t>}$
✓ Take Data as Requirements
✓ Rapid Development Process
BUT
× Black Box
× Vulnerable to confounding factors
2
Need for Domain-Aware DL Testing Models
Train Data
Data Preprocessing
Training Program
Learning Model
DNN Model
Test Data
Performance Testing
Model Testing
Domain Knowledge
λ serves to dynamically calibrate the magnitude of the adversarial loss to not overwhelm the original loss.
Original Data
Foreach $(X^{(b)}, y^{(b)})$
5
Pre-trained DNN
$loss_{orig}(X^{(b)}, y^{(b)}) + \lambda R_{phys}\left(\hat{X}^{(b)}_{adv}, D^{(b)}\right)$
7
Fine-tuned DNN
6
2
Physics-informed Adversarial Training
Foreach $x^{(i)}$
1
Sensitivity Rules
Foreach r_j
2
Deviation Function
Adversarial Examples
1 Foreach r_j
3
4 Store if True
Search Space Definition
3
Test Input Generation
Foreach valid $\hat{x}_{i,j}$
4
Adversarial Detection
3
Foreseeable Data Constraints
Physics-based Adversarial Testing
13
Physics-based Differential DL Testing
A Train a Sequential ML Model:
$f_{DL}(x) = \hat{y}_{DL}$
$\hat{y}$: DL Predictions
t
B Calibrate a PHYS Model: $f_{PHYS}(x) = \hat{y}_{phys}$
Estimate then:
i) Structural Uncertainty
ii) Parameters Uncertainty
iii) Experimental Uncertainty
$[c_{min}, c_{max}]$: PHYS Conf Intl
c_{max}
$\hat{y}_{avg}$
c_{min}
t
C
x_i: Altitude
x_j: Speed
t
Markovian Stochastic Process for Flight Generator
On-ground
descent
Climb
cruise
Fit Stochastic Generative Model for Feature Data Distribution
$P(x_i, x_j)$
D Assert that DL predictions are within the PHYS confidence intervals:
$\forall x, f_{DL}(x) = \hat{y}_{DL} \notin [c_{min}, c_{max}]$
$[x^{<t_s>}, x^{<t_s+m>}]$: Adversarial Region
t
t_s
$t_s + m$
It represents the adversarial input regions for which the predictions are not consistent with the physics-based model.
19