Robust and Rapid Adaption for Concept Drift in Software System Anomaly Detection

Minghua Ma, Shenglin Zhang, Dan Pei,

Xin Huang, Hongwei Dai

ISSRE 2018

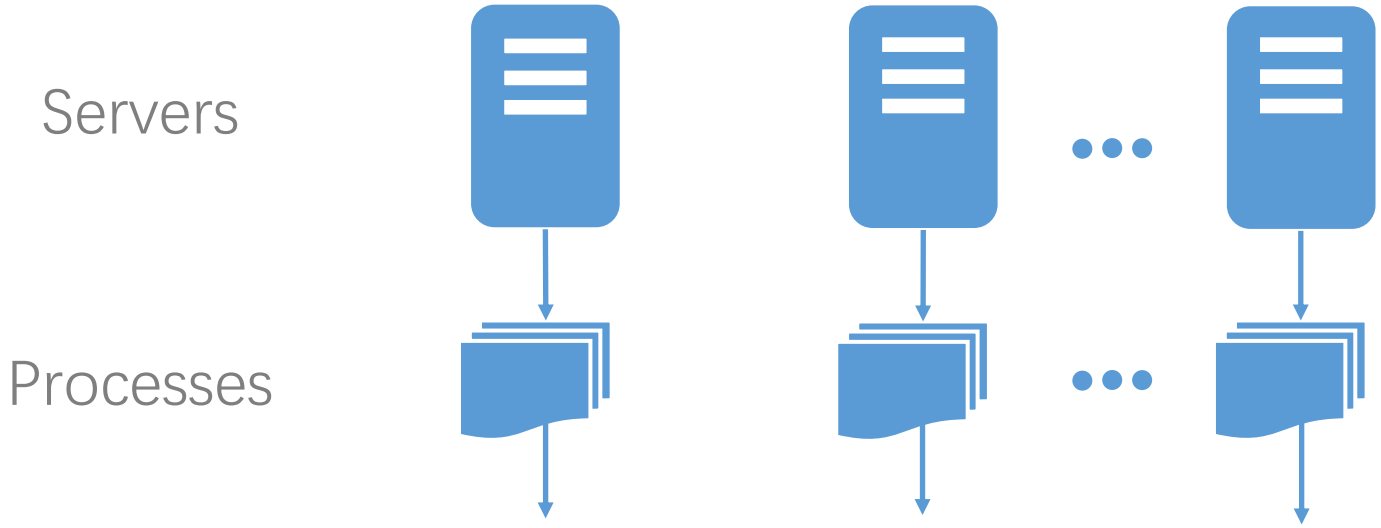
Web-based Software System

Search Engine

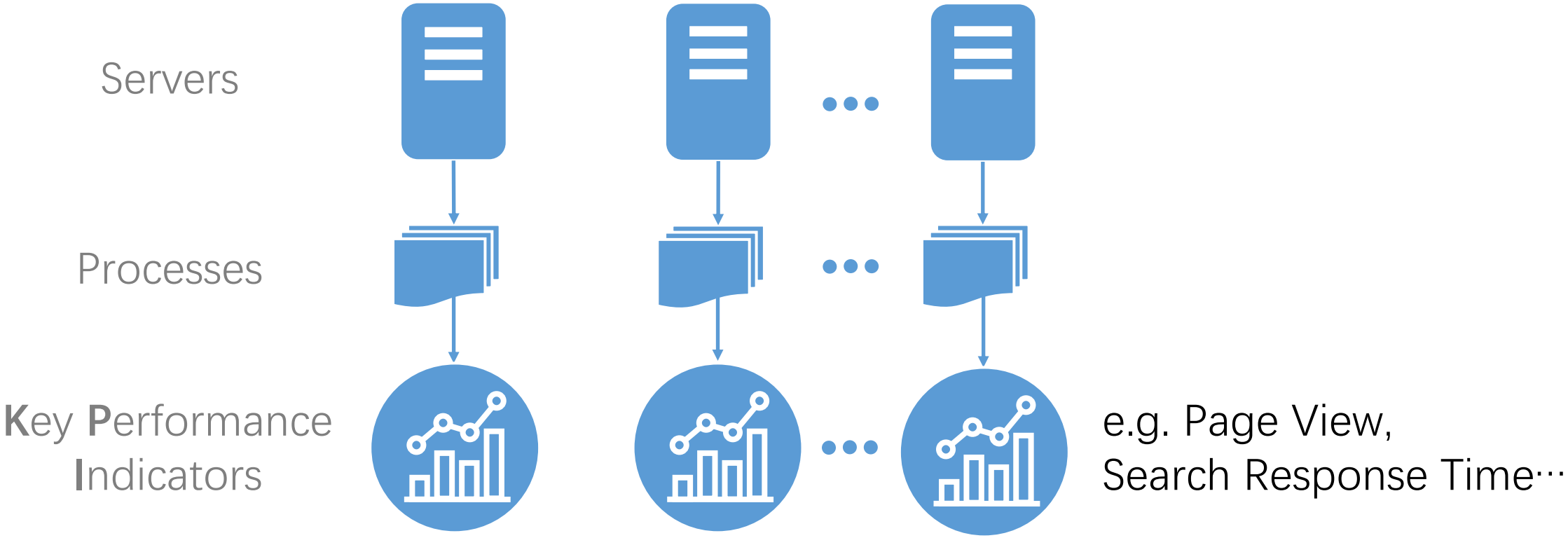
Online Shopping

Social Network

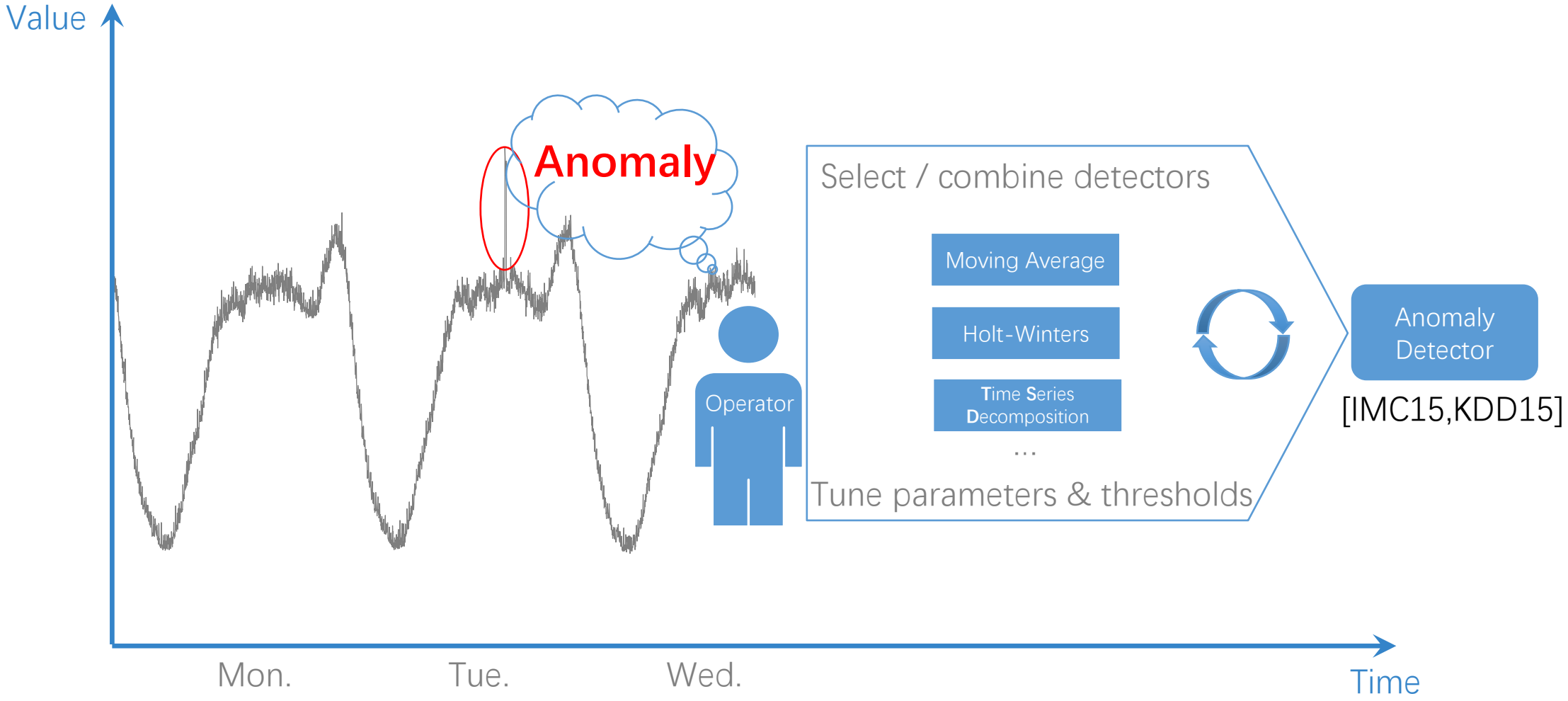
Web-based Software System Measurements



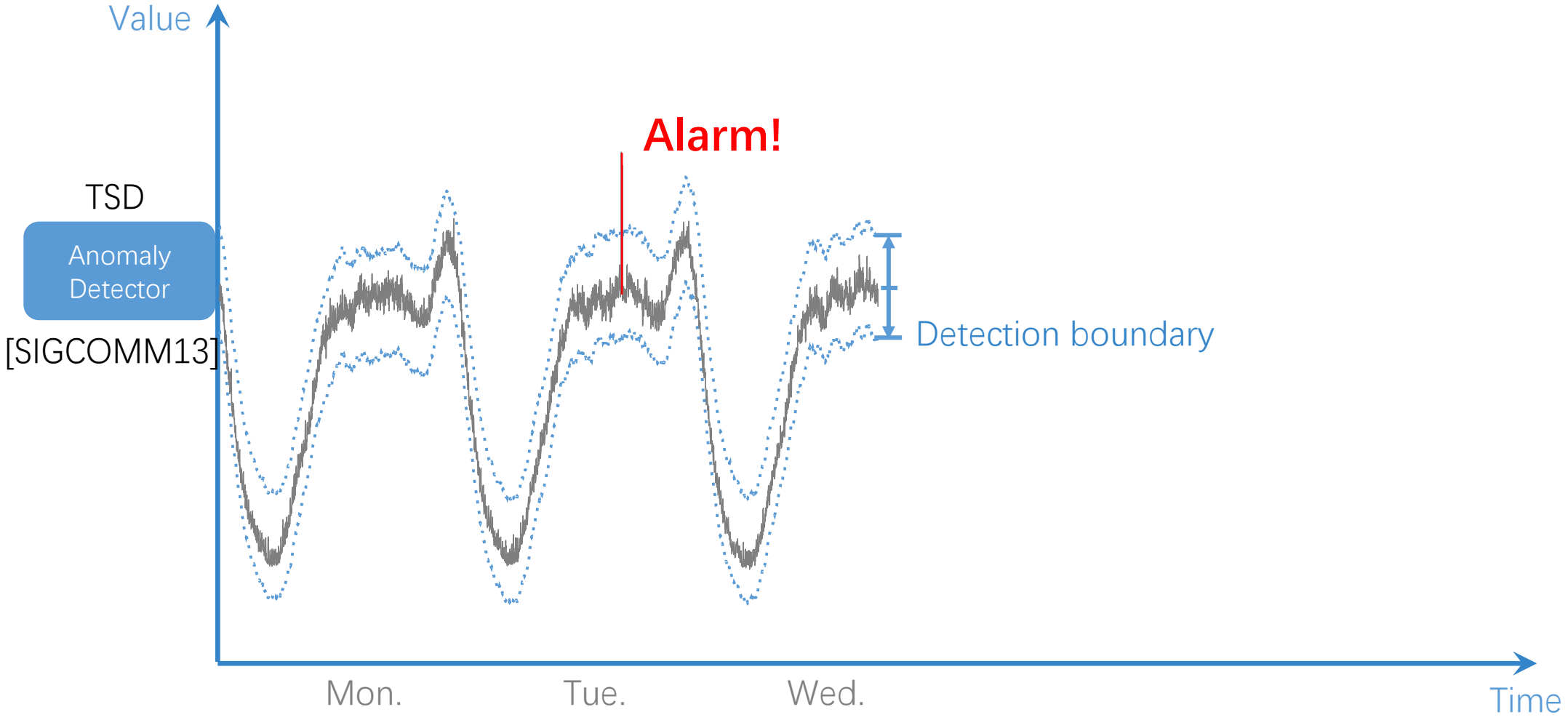
Web-based Software System Measurements



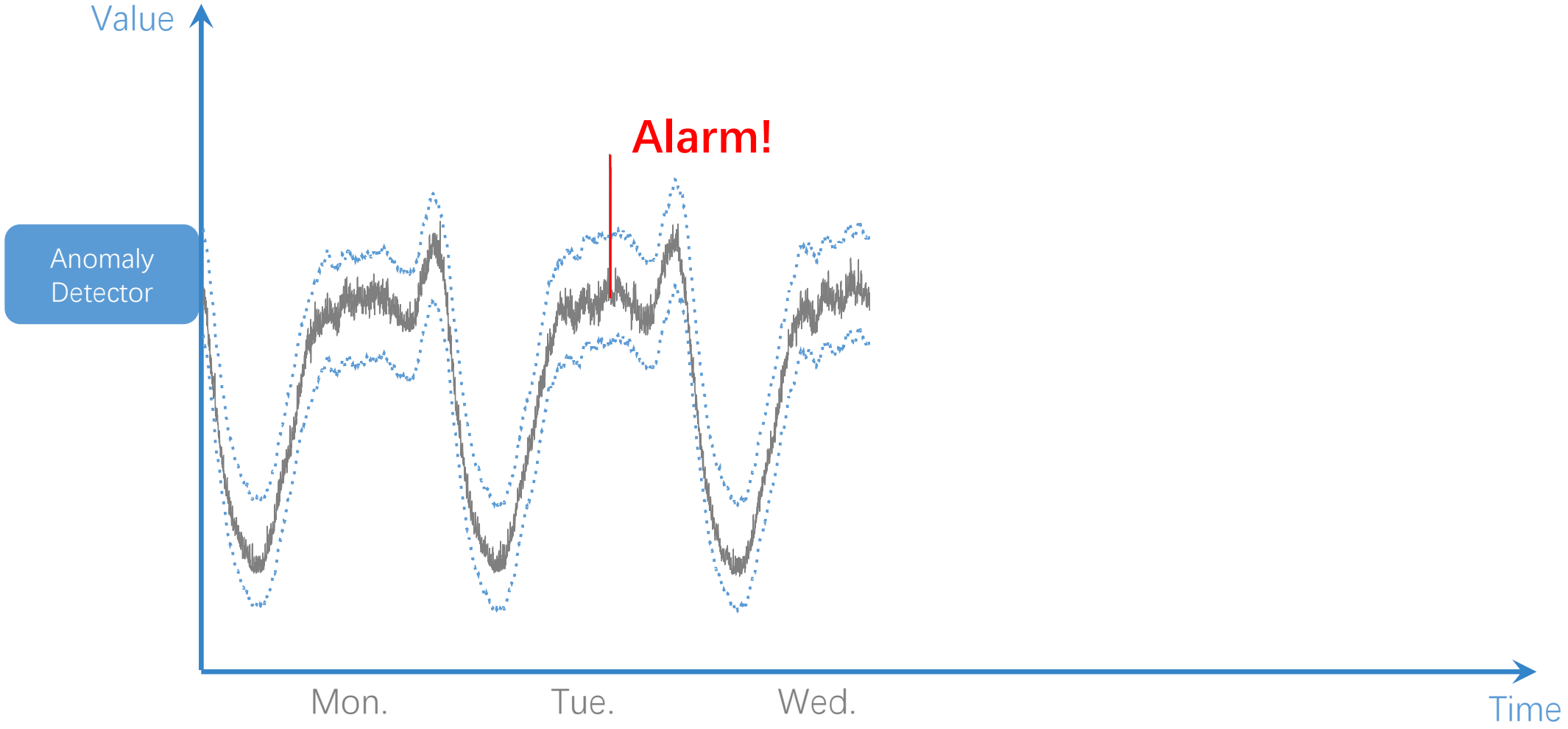
How to Build an Anomaly Detector



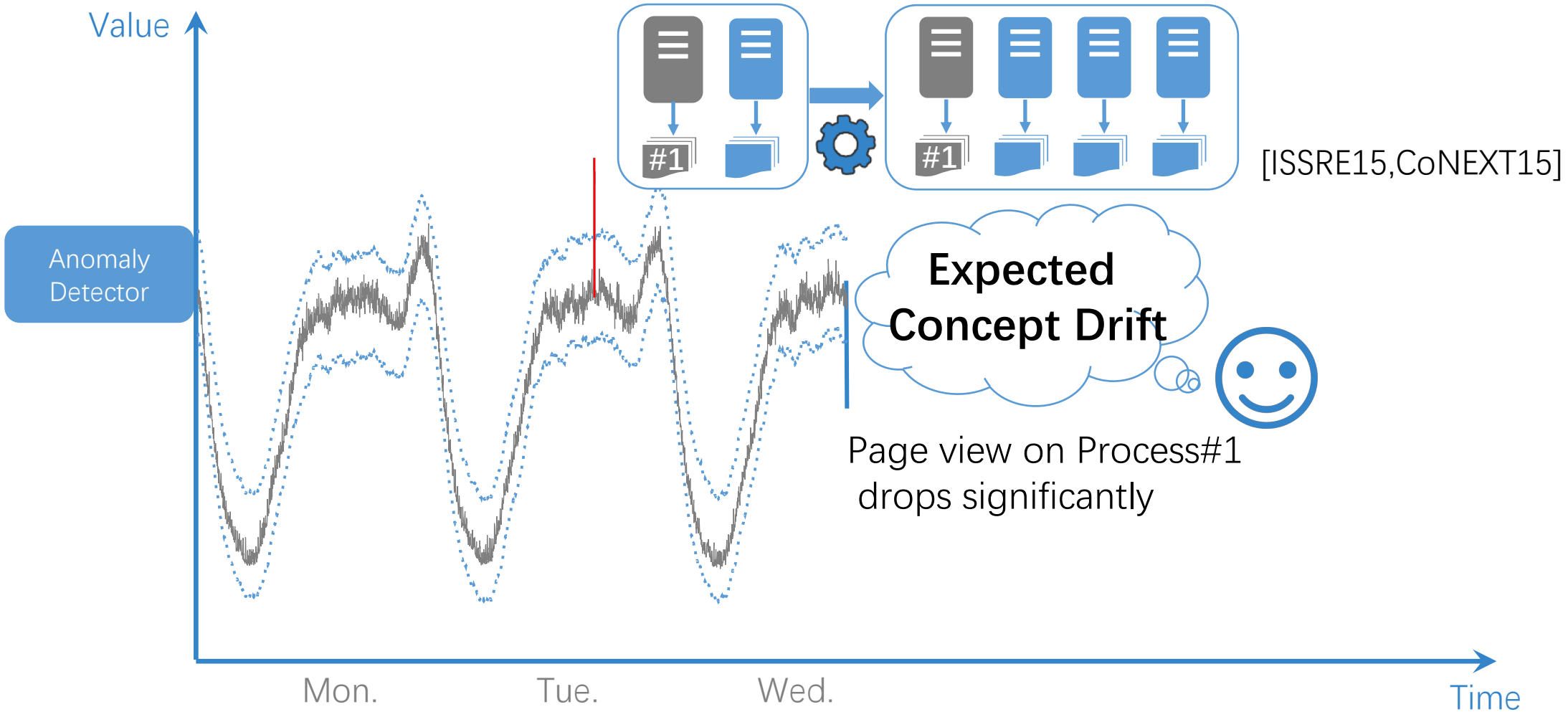
How Anomaly Detector Works



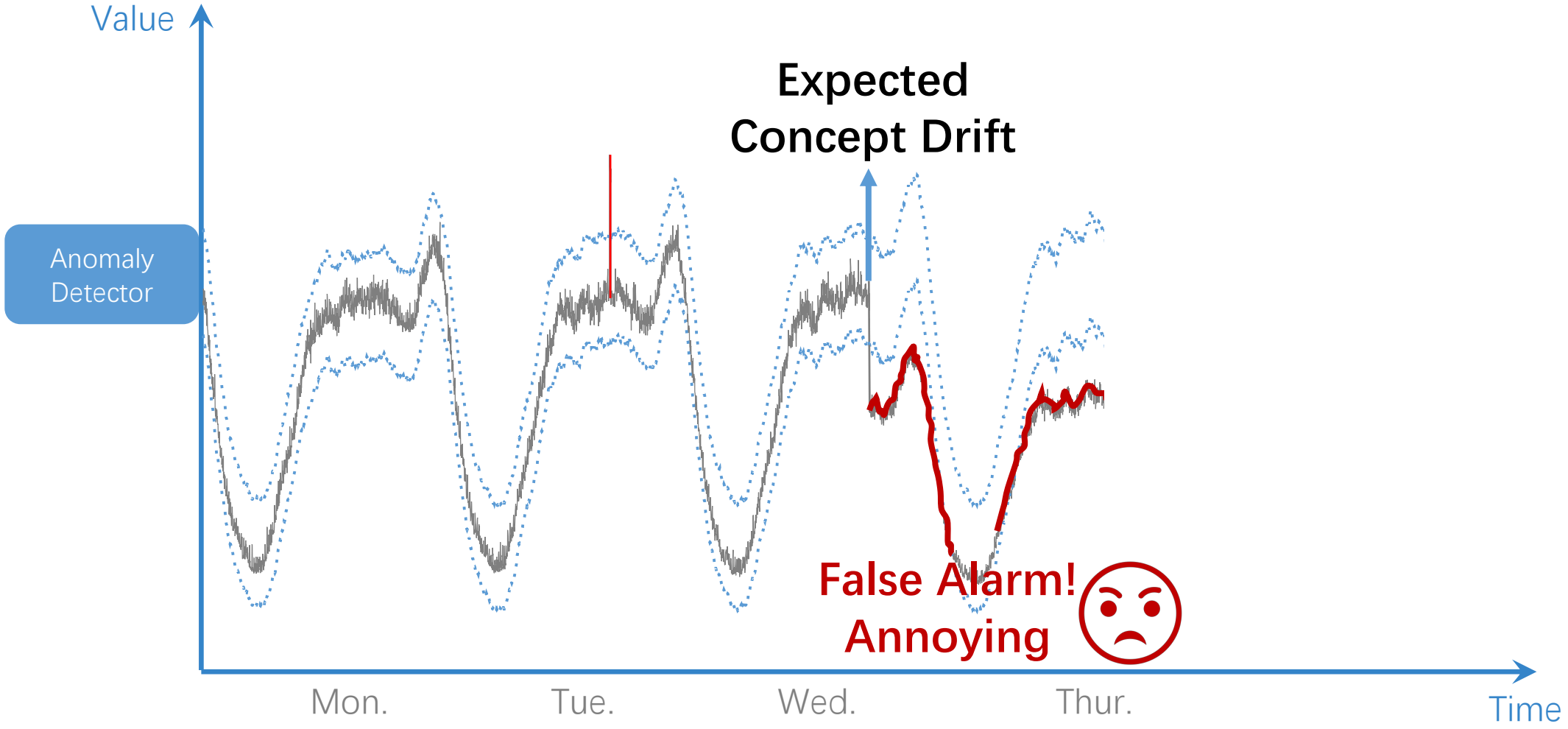
Operators Often Conduct Software Changes



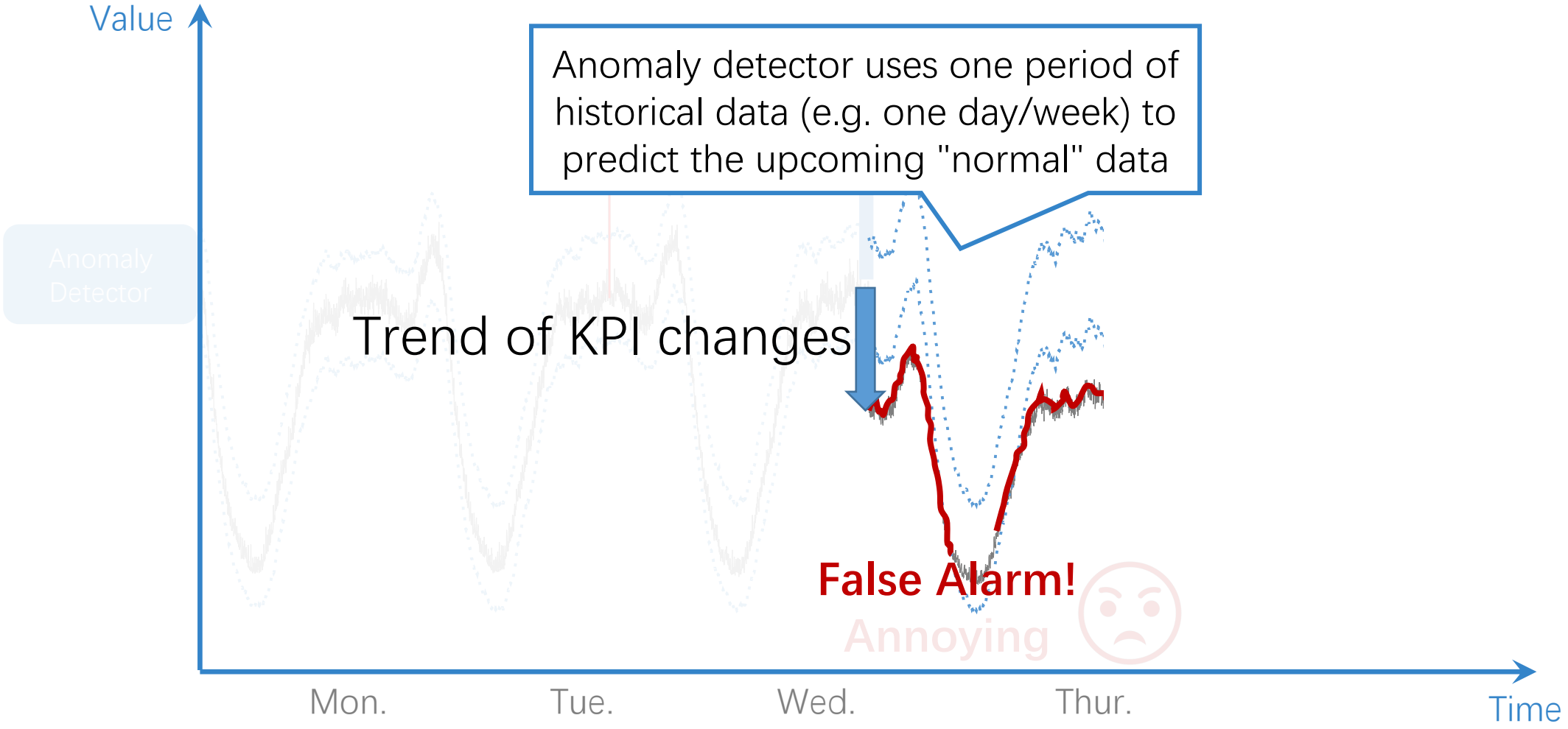
Operators Often Conduct Software Changes



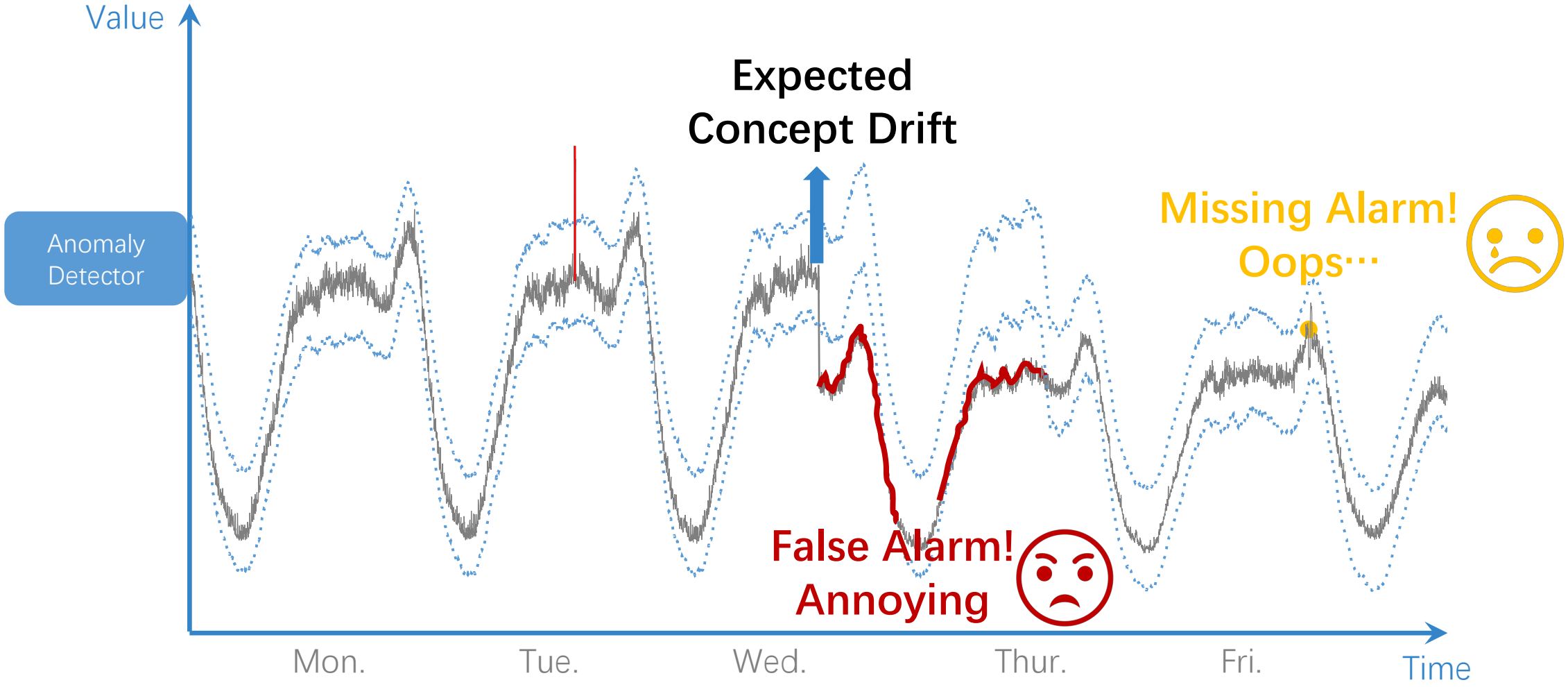
Accuracy of Anomaly Detector Degrades



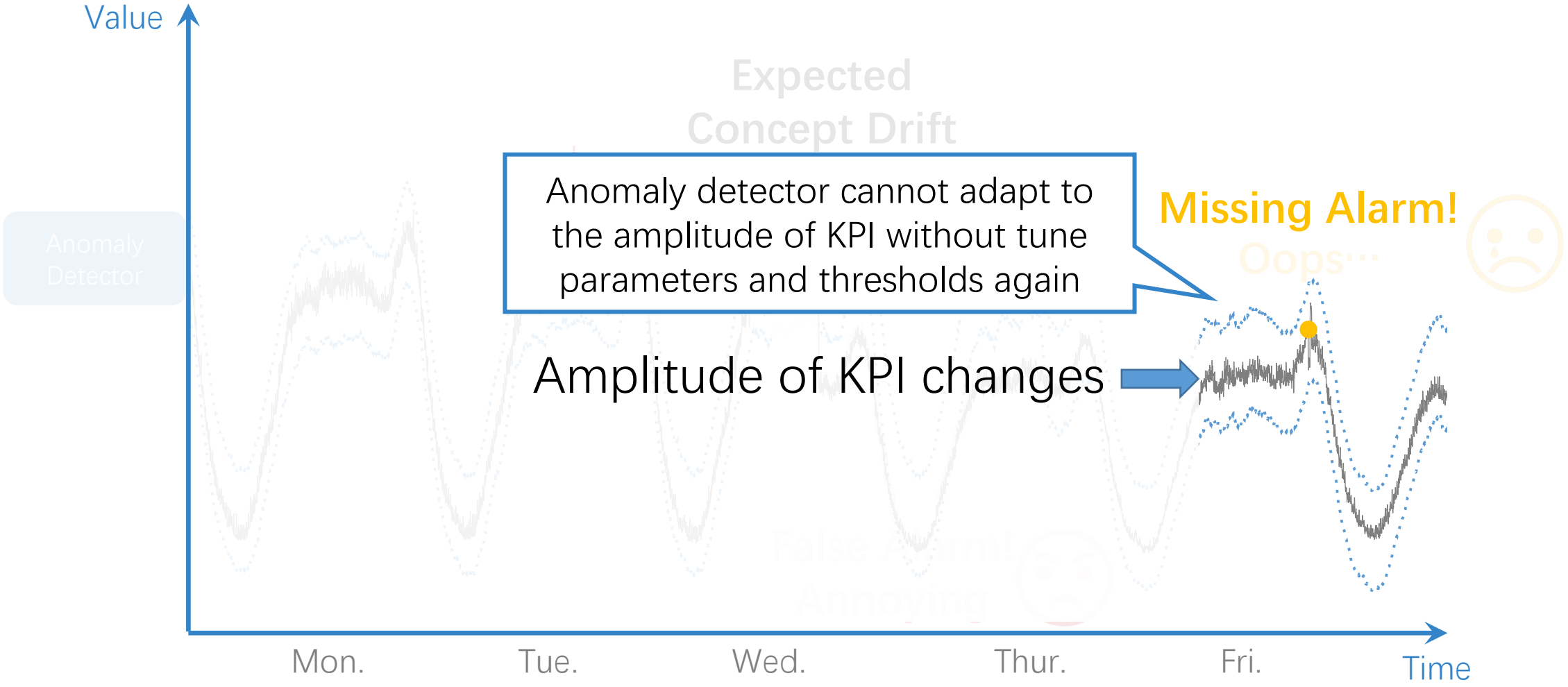
Accuracy Degradation Reason #1: False Alarm



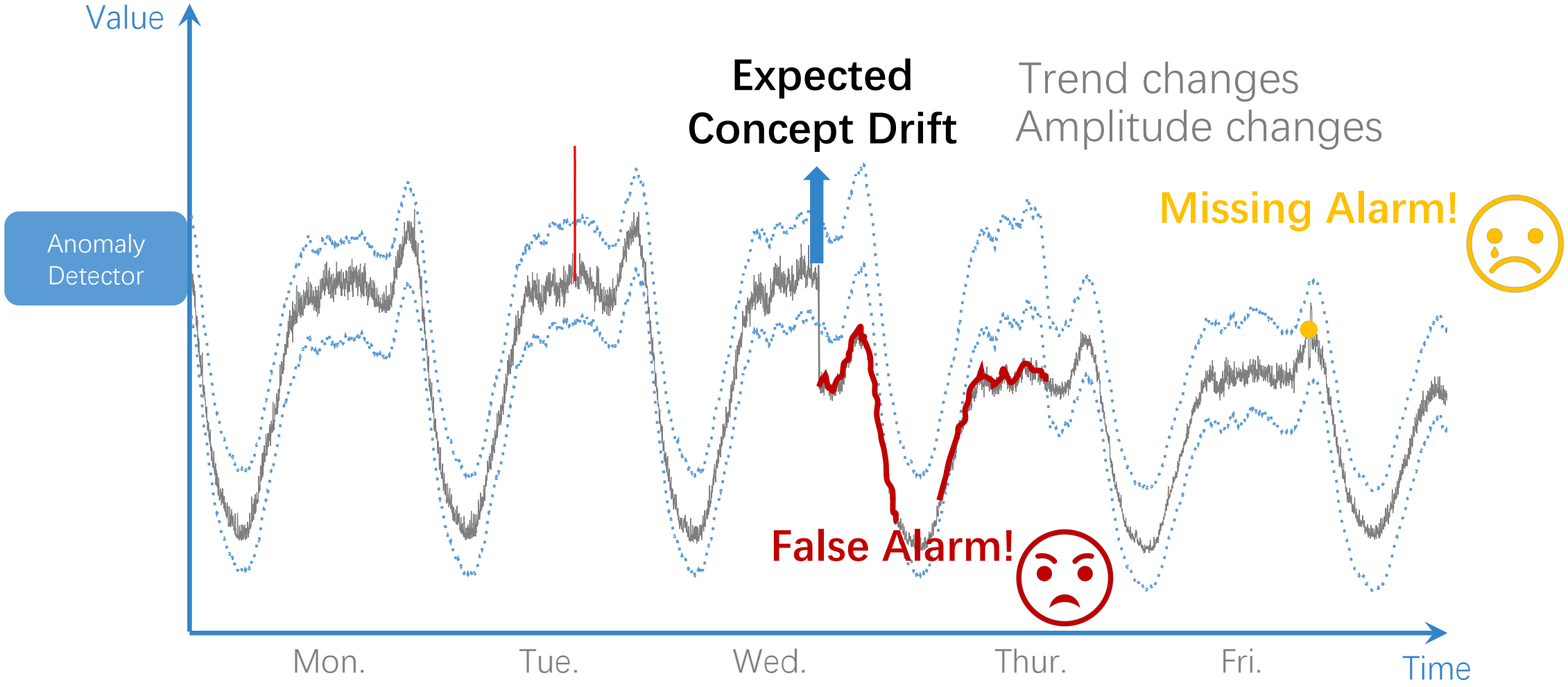
Accuracy of Anomaly Detectors Degrade



Accuracy Degradation Reason #2: Missing Alarm



Accuracy of Anomaly Detectors Degrade



Outline

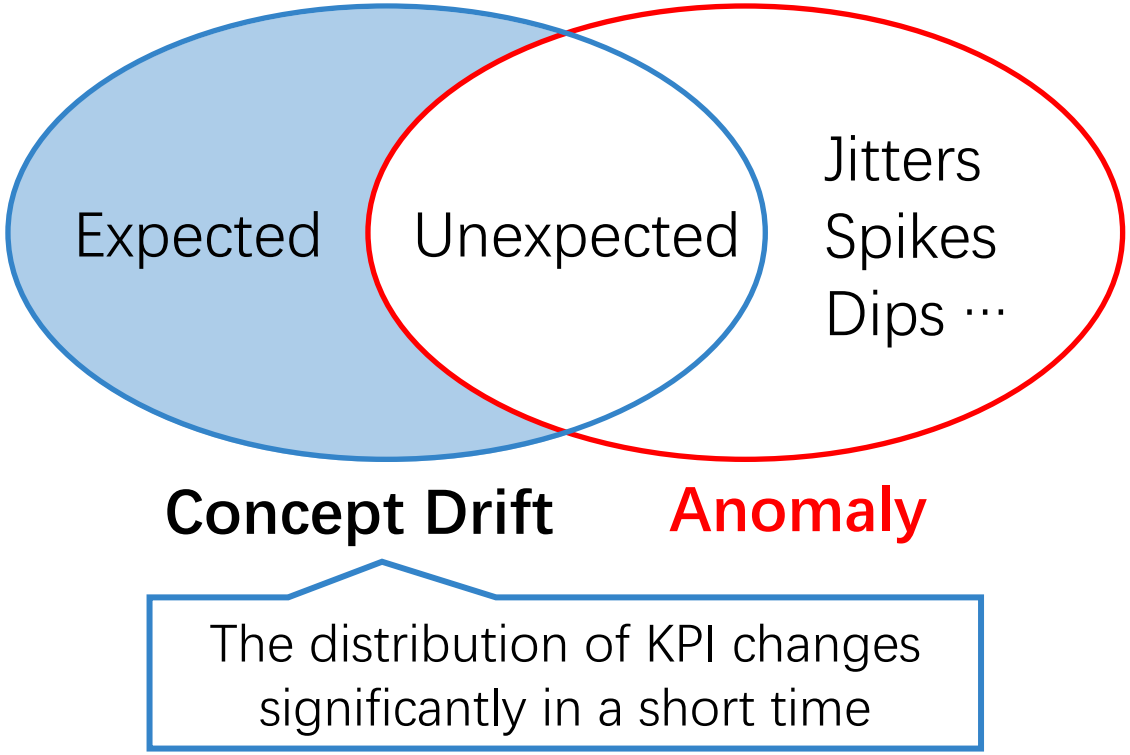
What's concept drift?

Why it's challenging?

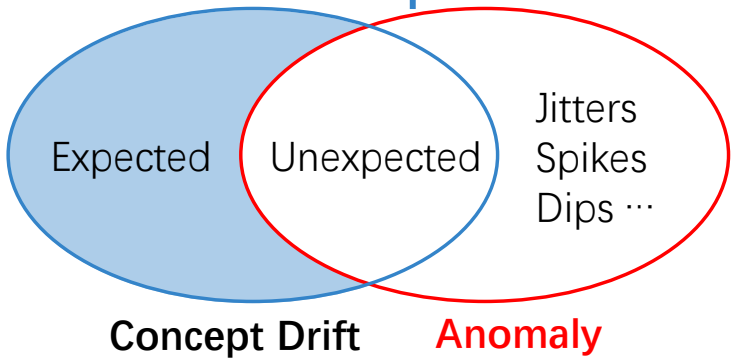
How to adapt to it?

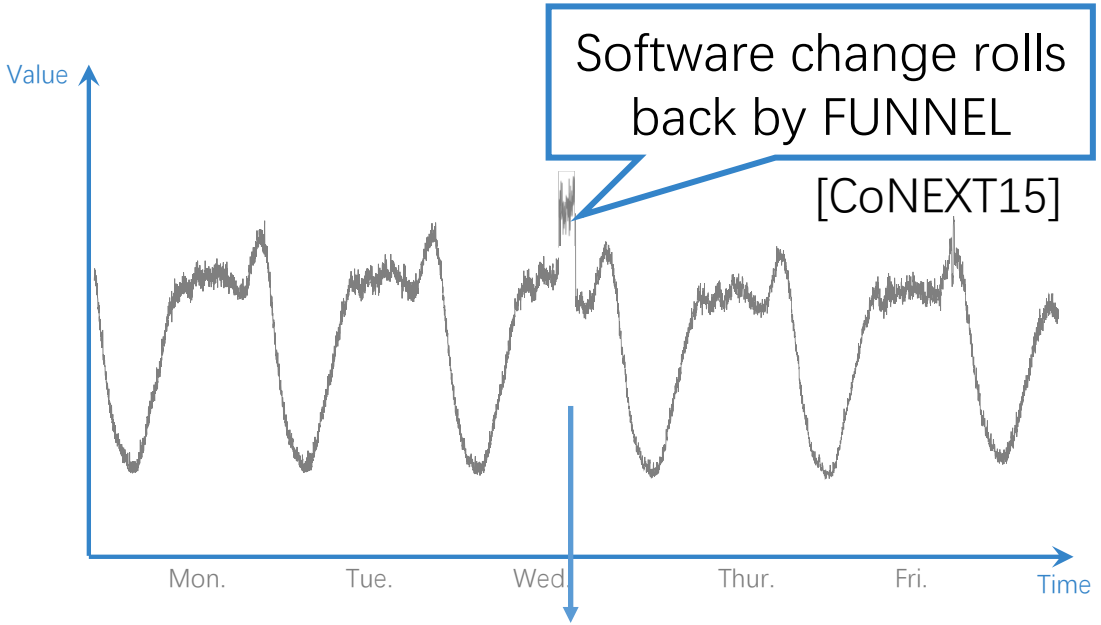
Evaluation

Concept Drift in KPI Anomaly Detection



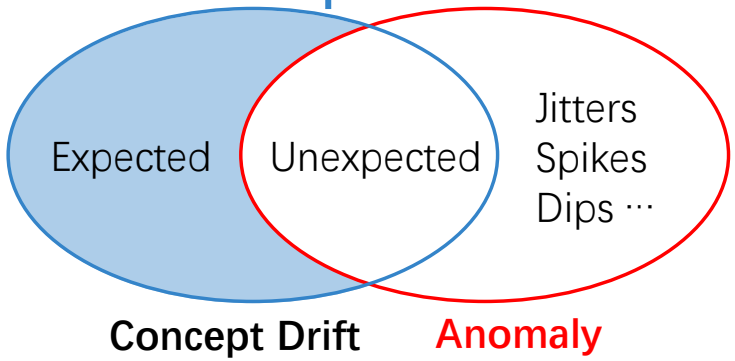
Unexpected Concept Drift: Roll Back

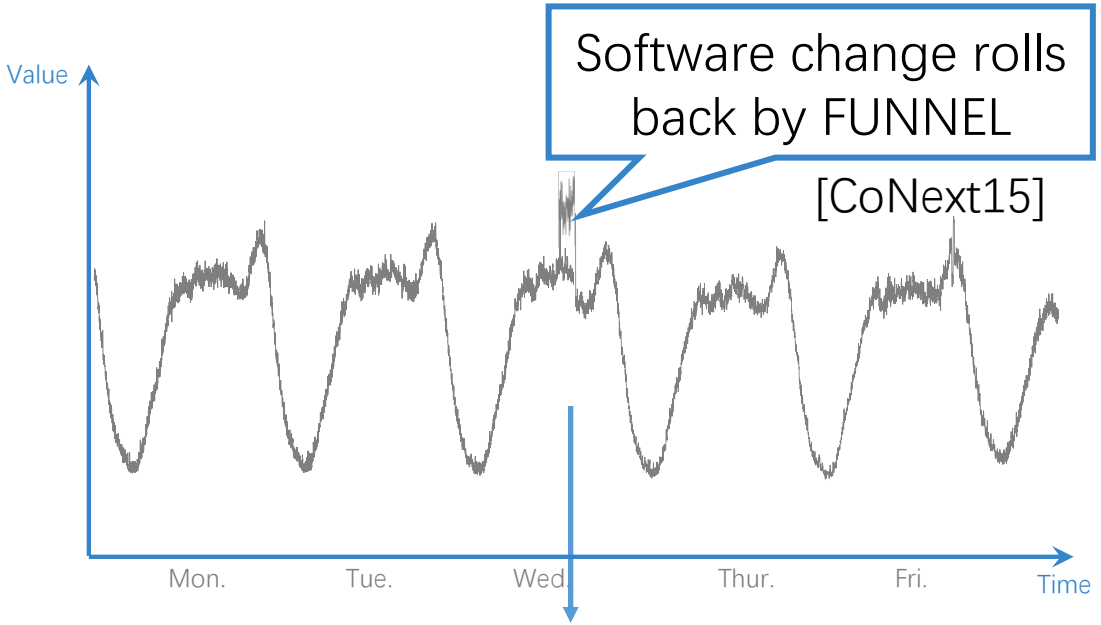




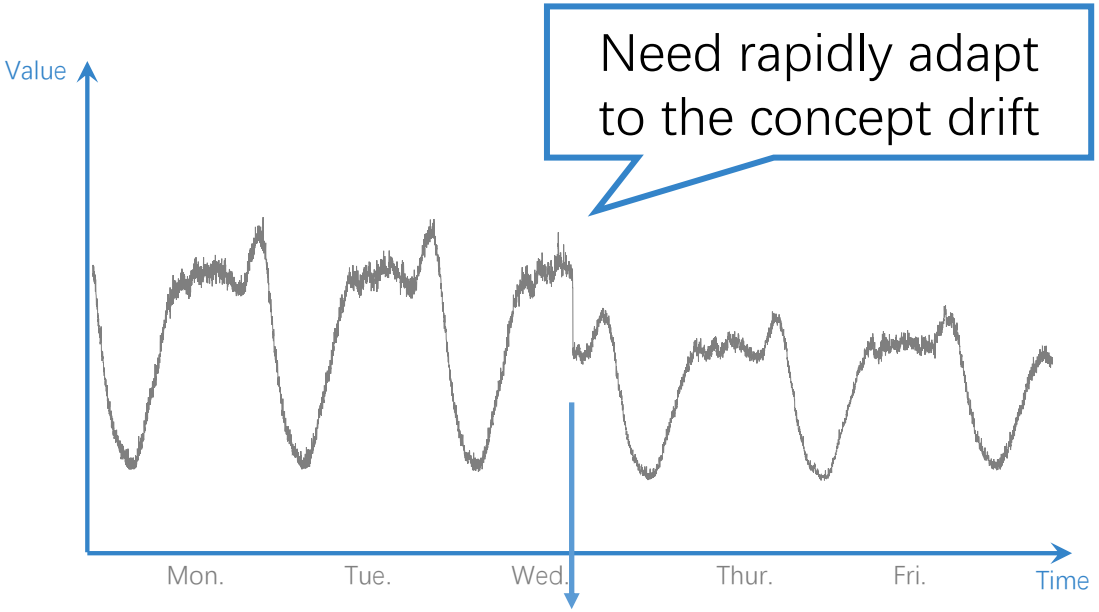
Unexpeceted concept drift

Expected Concept Drift: Our Focus





Unexpeceted concept drift



Expeceted concept drift

Outline

What's concept drift? ➔ KPI distribution change

Why it's challenging?

How to adapt to it?

Evaluation

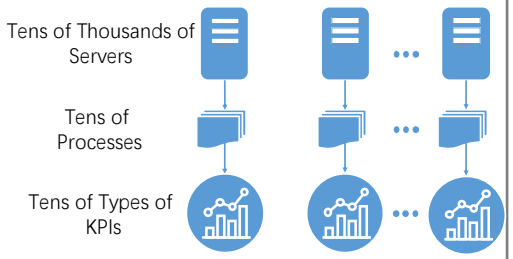
Why Is Adaption to Concept Drift Challenging

搜狗搜索

3000 Concept Drifts Per Day

80% Are Expected Ones

High Frequency



Huge Amount of KPIs

Single Detectors or Combination

Diverse Detectors

Rapid Adaptio

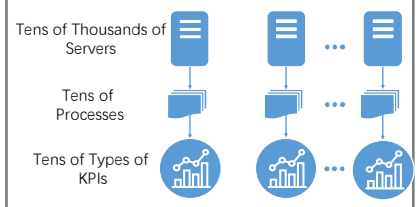
Why Is Adaption to Concept Drift Challenging

搜狗搜索

3000 Concept Drifts Per Day

80% Are Expected Ones

High Frequency



Huge Amount of KPIs

Diverse Detectors

Rapid Adaption

➔ Need an **automatic** concept drift adaption approach

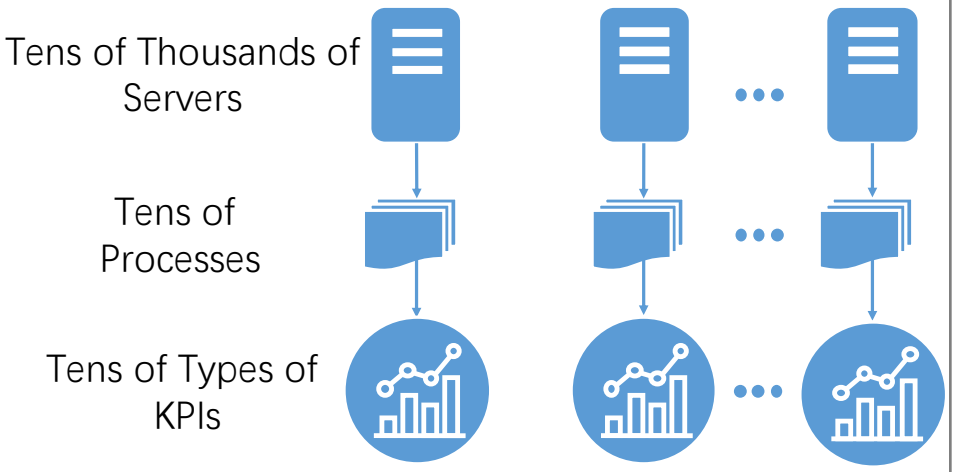
Why Is Adaption to Concept Drift Challenging

搜狗搜索

3000 Concept Drifts Per Day

80% Are Expected Ones

High Frequency



Huge Amount of KPIs

Single Detectors or Combination

Diverse Detectors

Rapid Adaption

[CoNext15, IMC15]

➔ Cannot **tune parameters manually** for each KPI stream

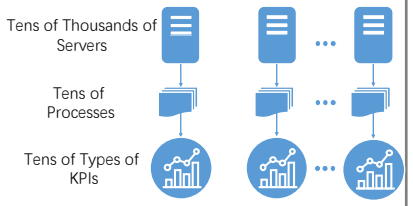
Why Is Adaption to Concept Drift Challenging

搜狗搜索

3000 Concept Drifts Per Day

80% Are Expected Ones

High Frequency



Huge Amount of KPIs

Single Detectors or Combination

Diverse Detectors

[IMC15, SIGCOMM10, SIGCOMM13]

Rapid Adaption

➔ Need a **generic** adaption approach for various types of detectors

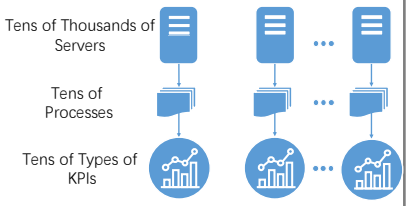
Why Is Adaption to Concept Drift Challenging

搜狗搜索

3000 Concept Drifts Per Day

80% Are Expected Ones

High Frequency



Huge Amount of KPIs

Single Detectors or Combination

Diverse Detectors

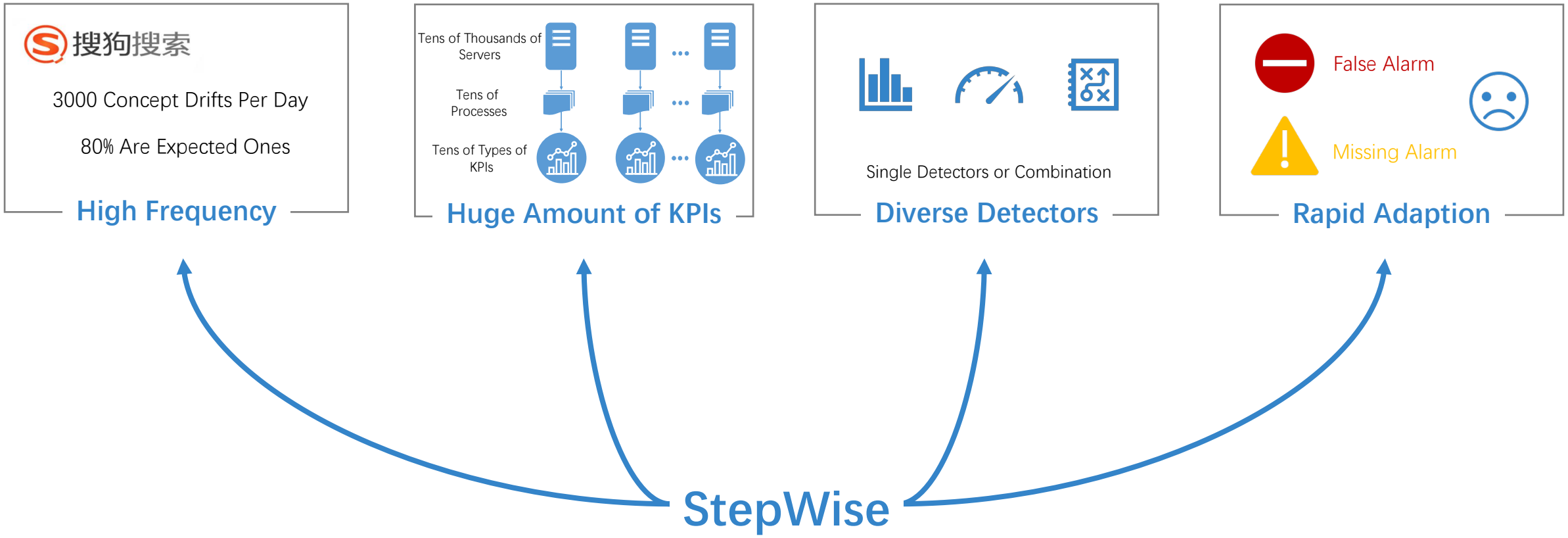
False Alarm

Missing Alarm

Rapid Adaption

➔ Help anomaly detectors adapt concept drift in a **rapid** manner

Why Is Adaption to Concept Drift Challenging



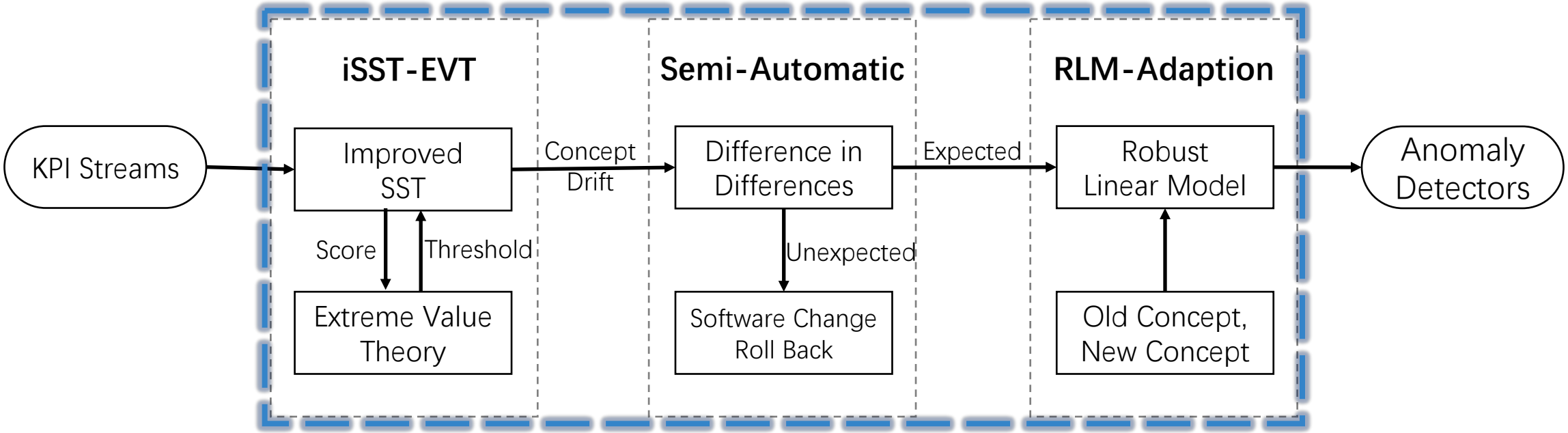
StepWise

Detection, Classification and Adaption

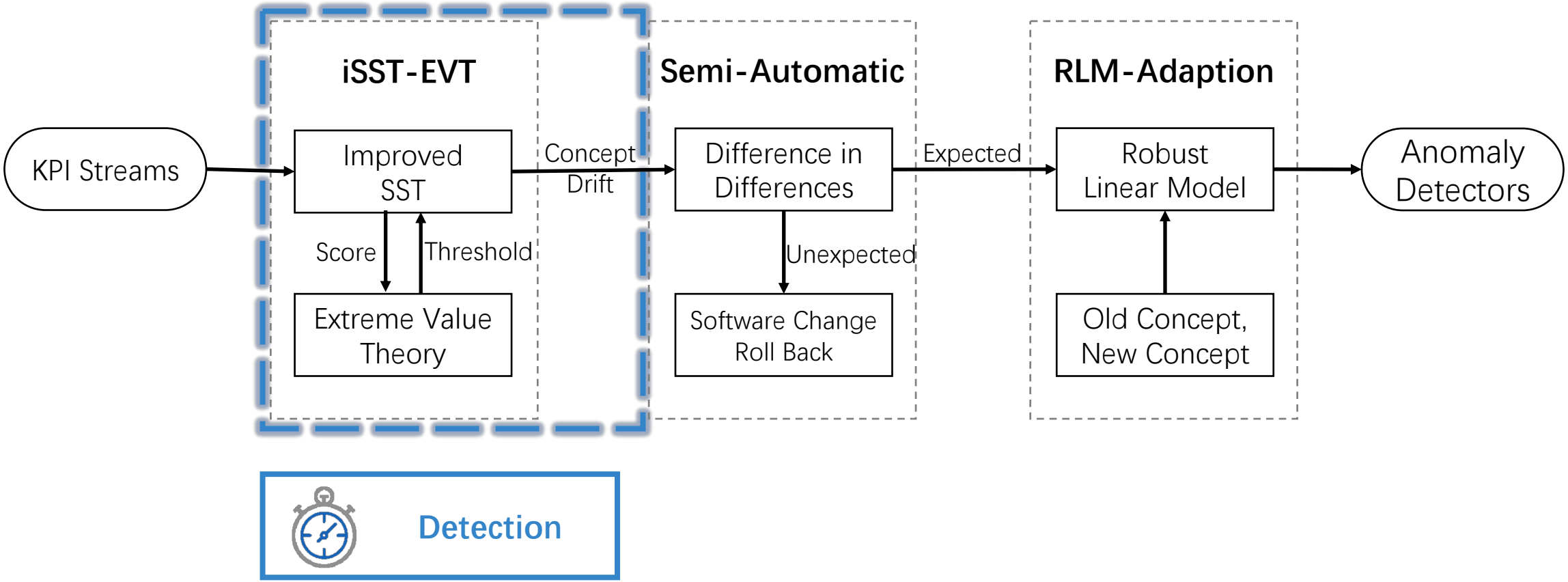
Concept Drift

in Software System Anomaly Detection

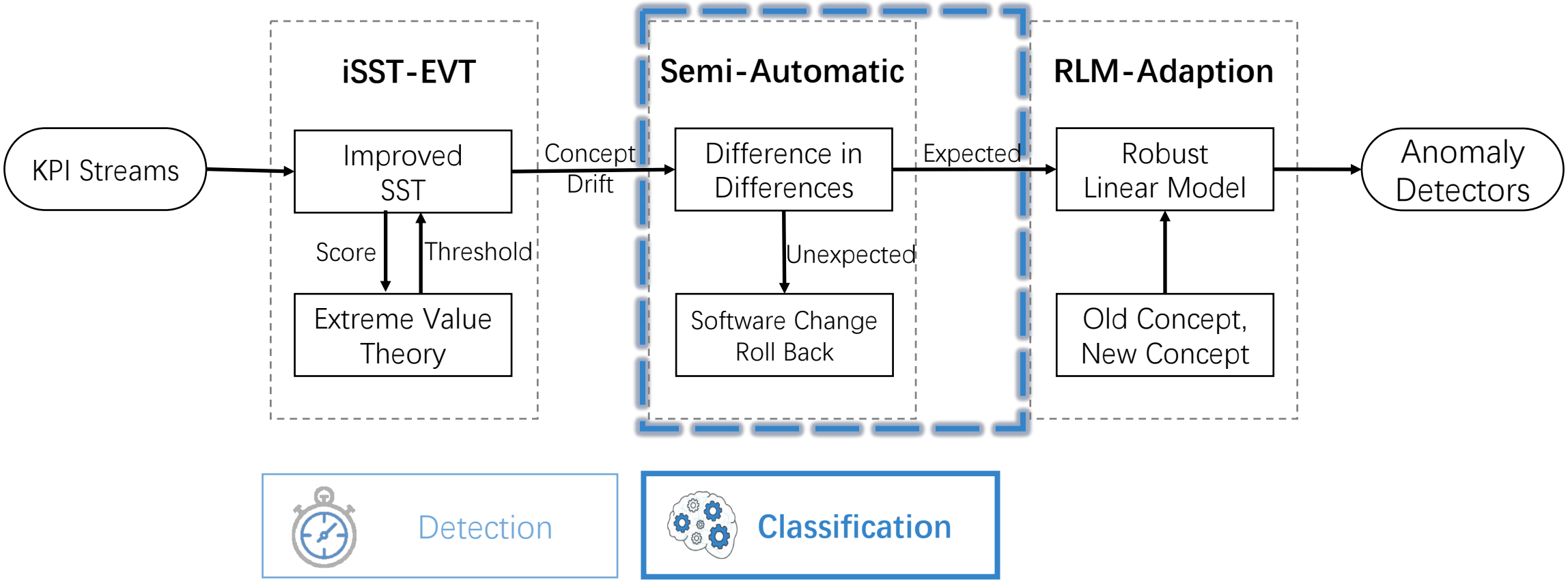
StepWise Overview



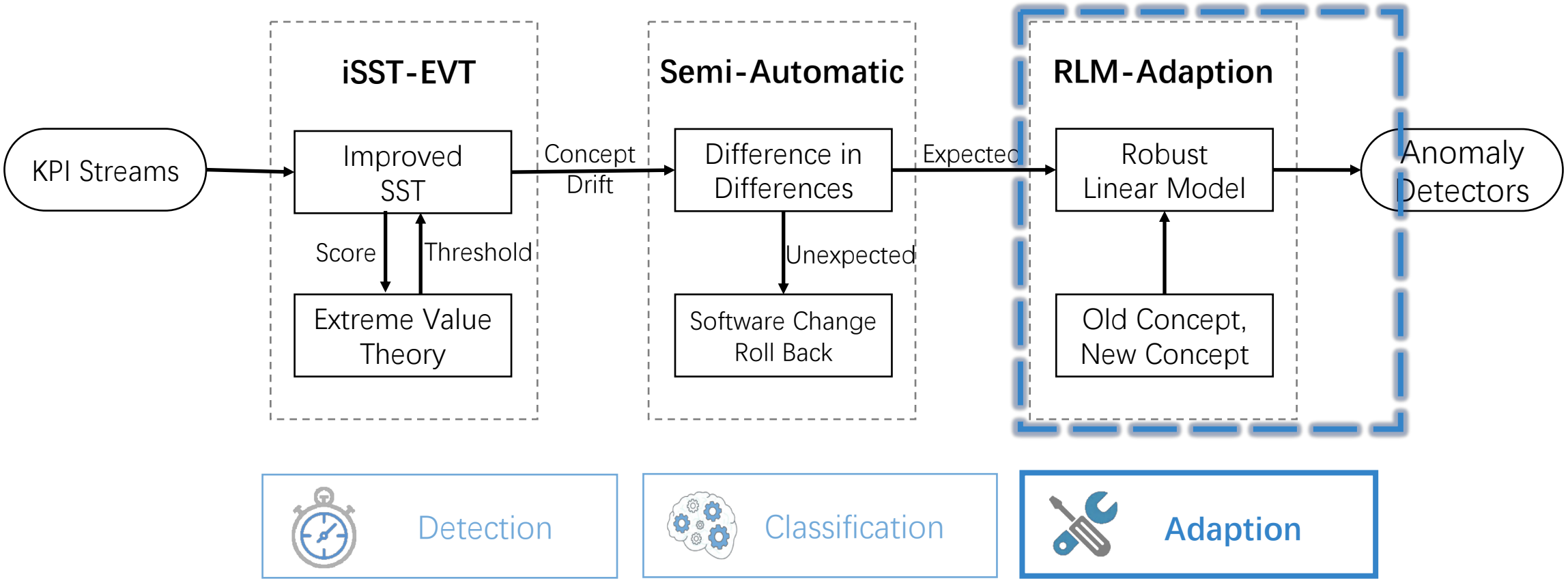
StepWise Overview



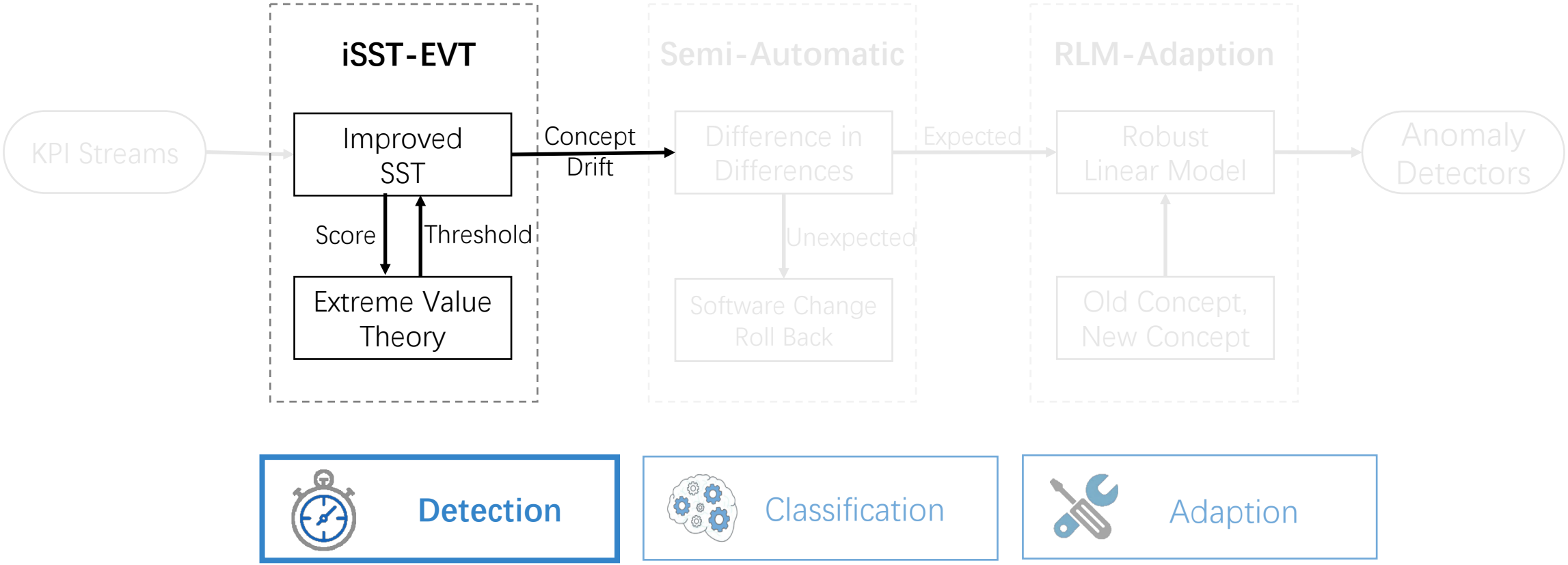
StepWise Overview



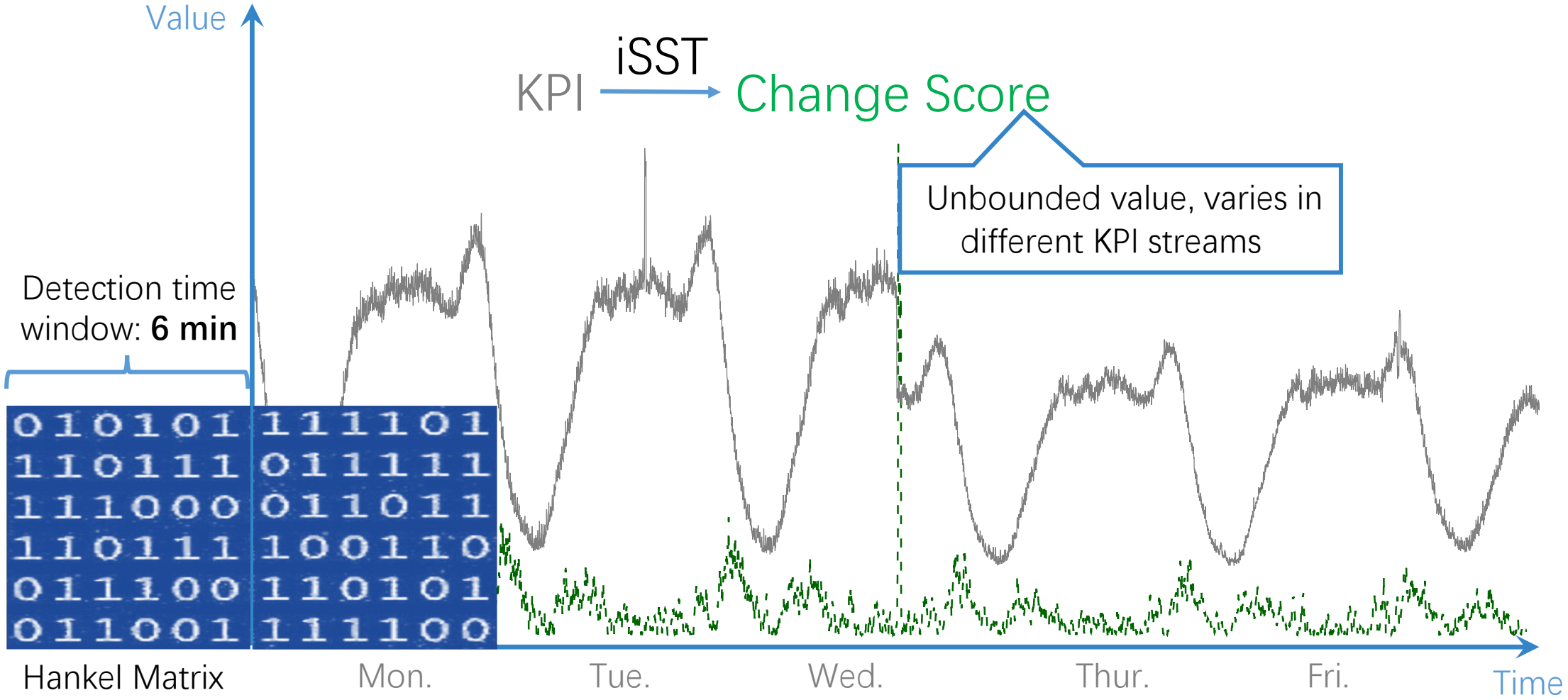
StepWise Overview



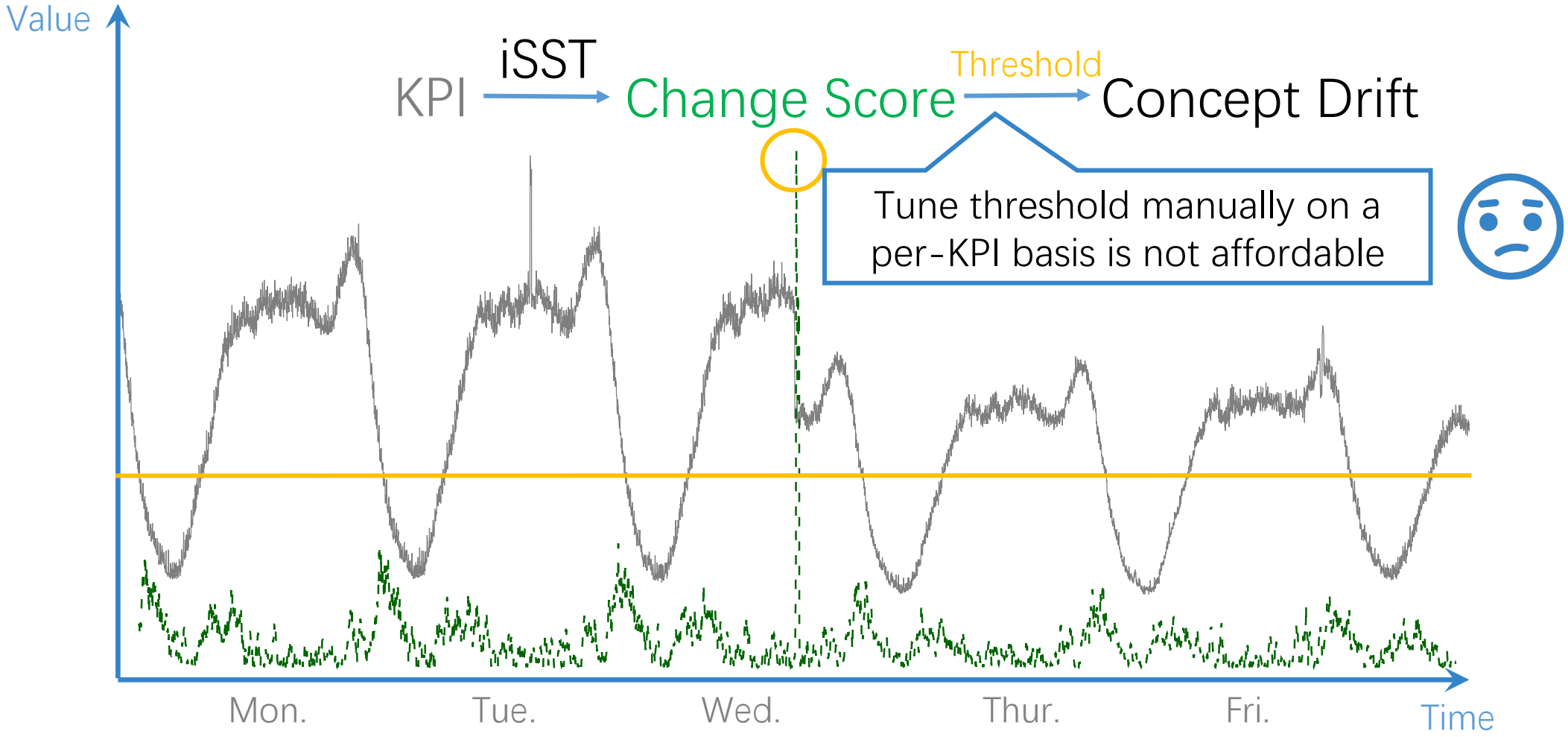
iSST-EVT Detection



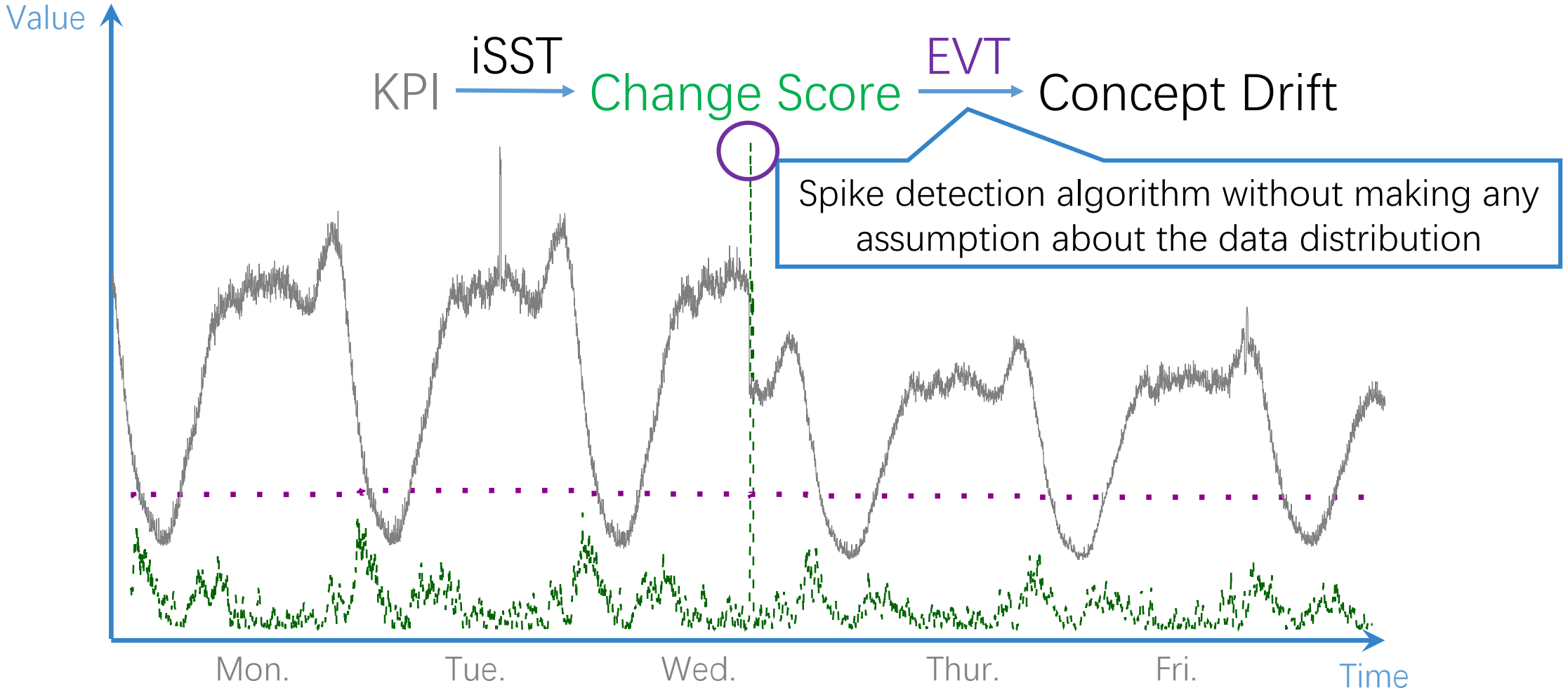
iSST: Improved Singular Spectrum Transform



iSST: Improved Singular Spectrum Transform



Idea #1. iSST-EVT



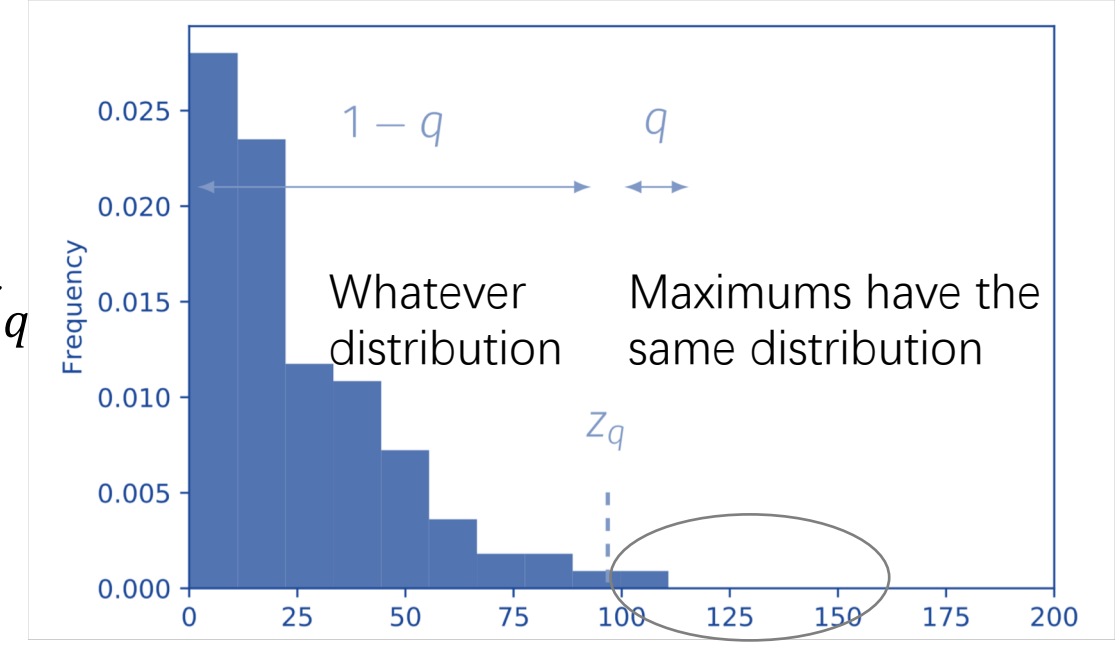
EVT: Extreme Value Theory

Extreme Value Distribution $G_\gamma : x \mapsto \exp(-(1+\gamma x)^{-\frac{1}{\gamma}})$

[KDD17]

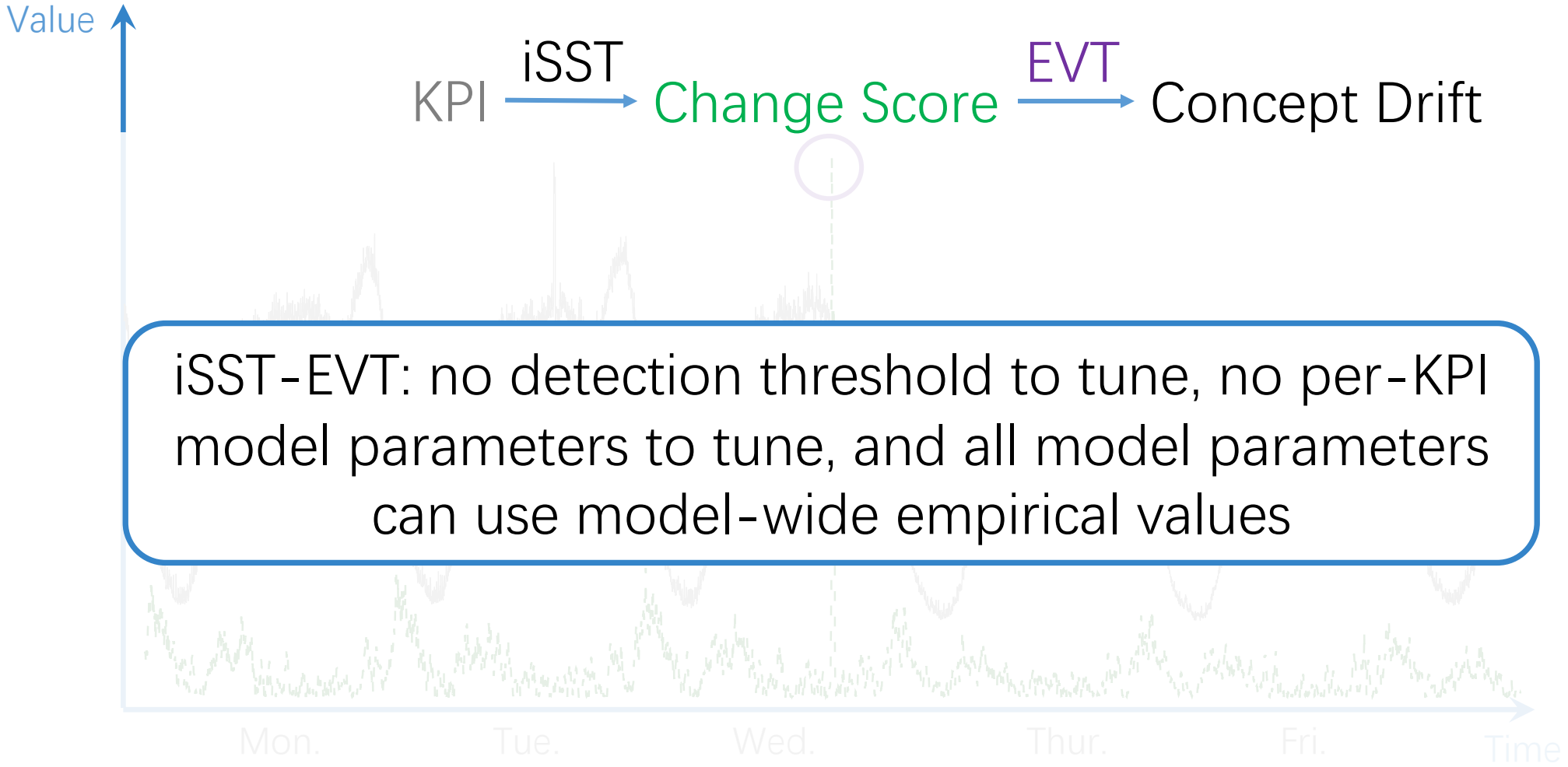
Change score

$X_1, X_2, \ldots, X_n$ → EVT ← q → z_q



Compute z_q such as $\mathbb{P}(X > z_q) < q$

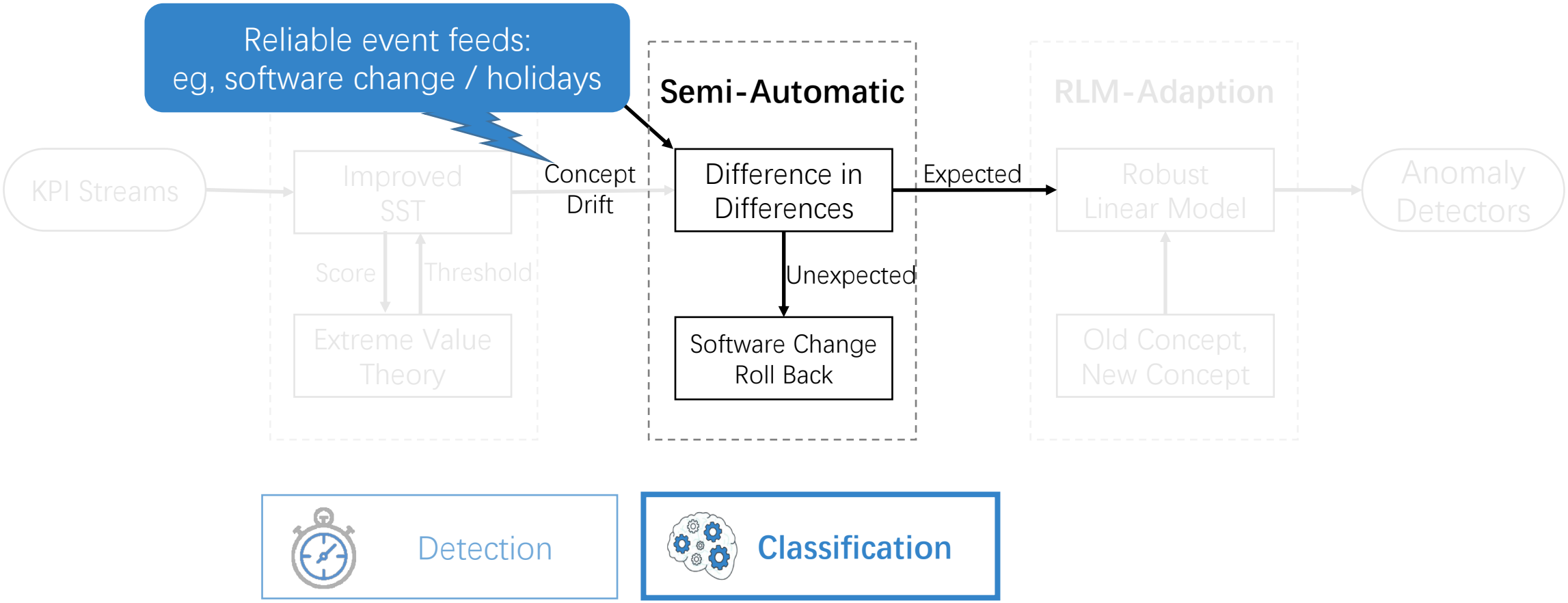
Idea #1. iSST-EVT



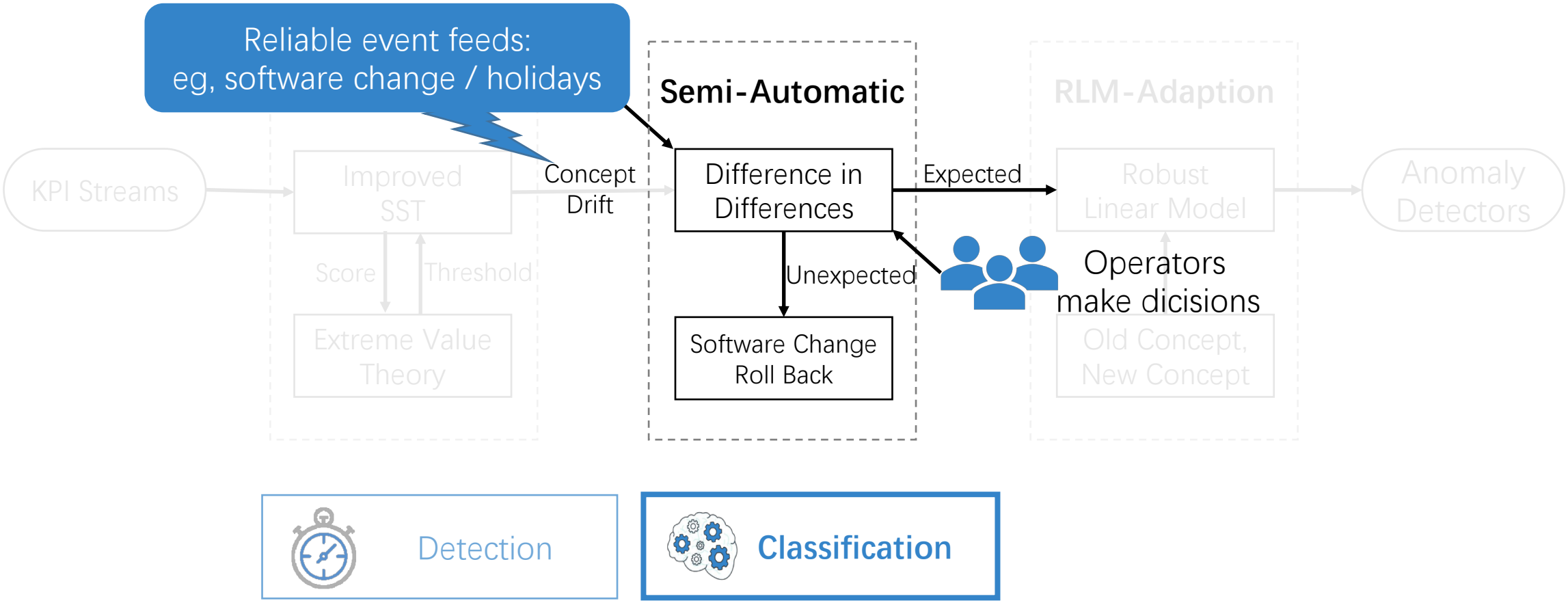
KPI $\xrightarrow{\text{iSST}}$ Change Score $\xrightarrow{\text{EVT}}$ Concept Drift

iSST-EVT: no detection threshold to tune, no per-KPI model parameters to tune, and all model parameters can use model-wide empirical values

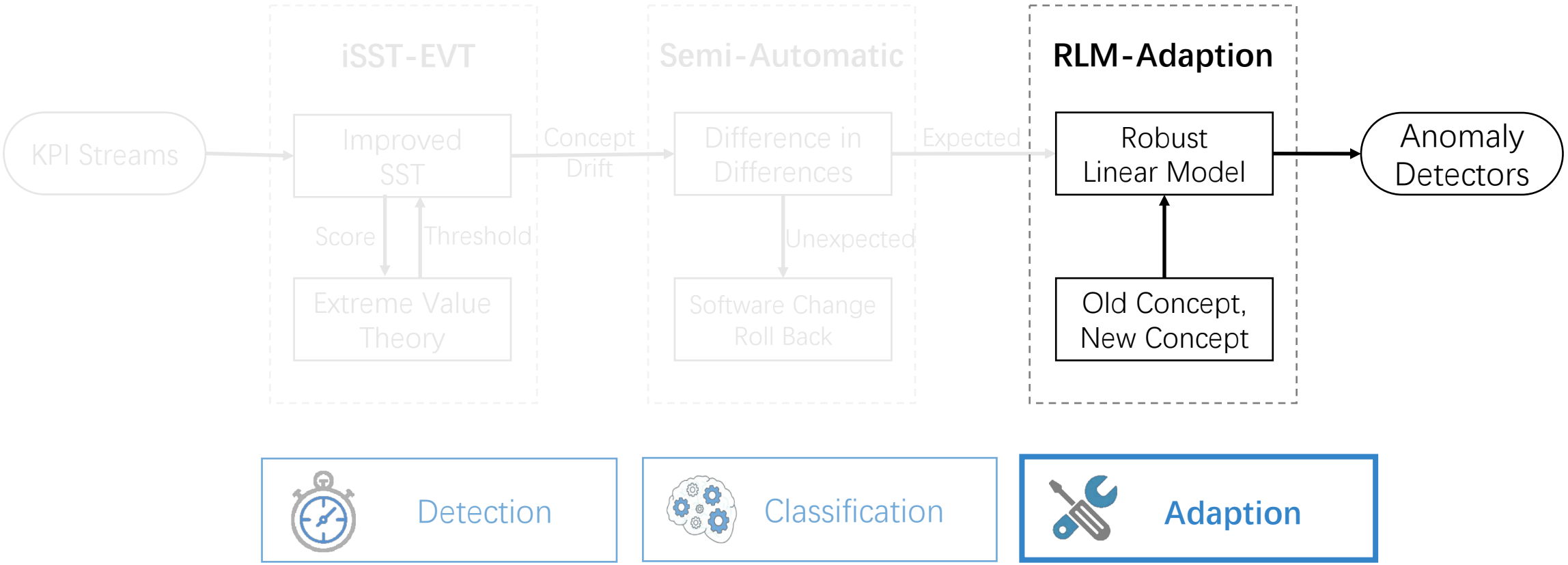
Semi-Automatic Classification



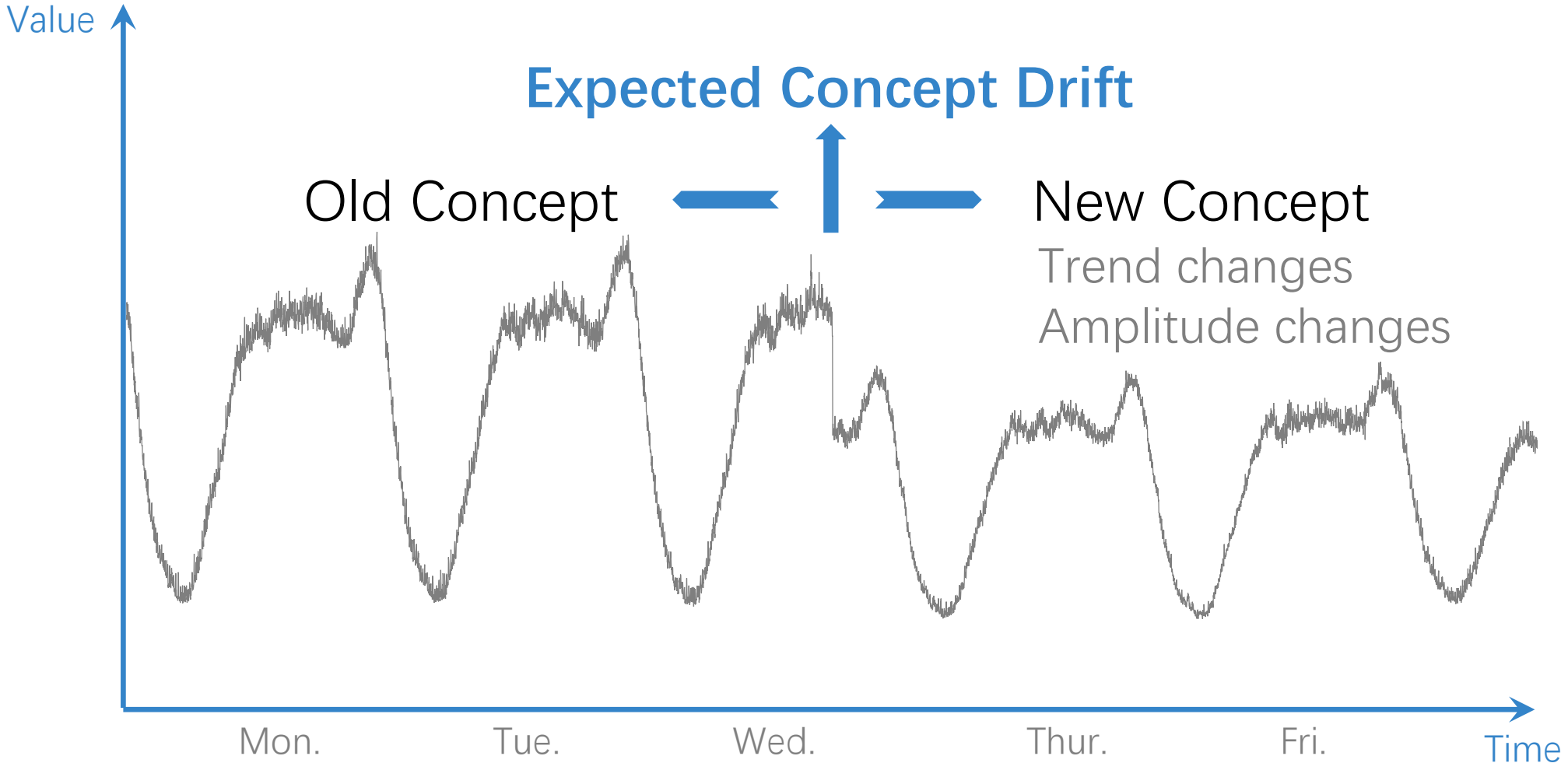
Semi-Automatic Classification



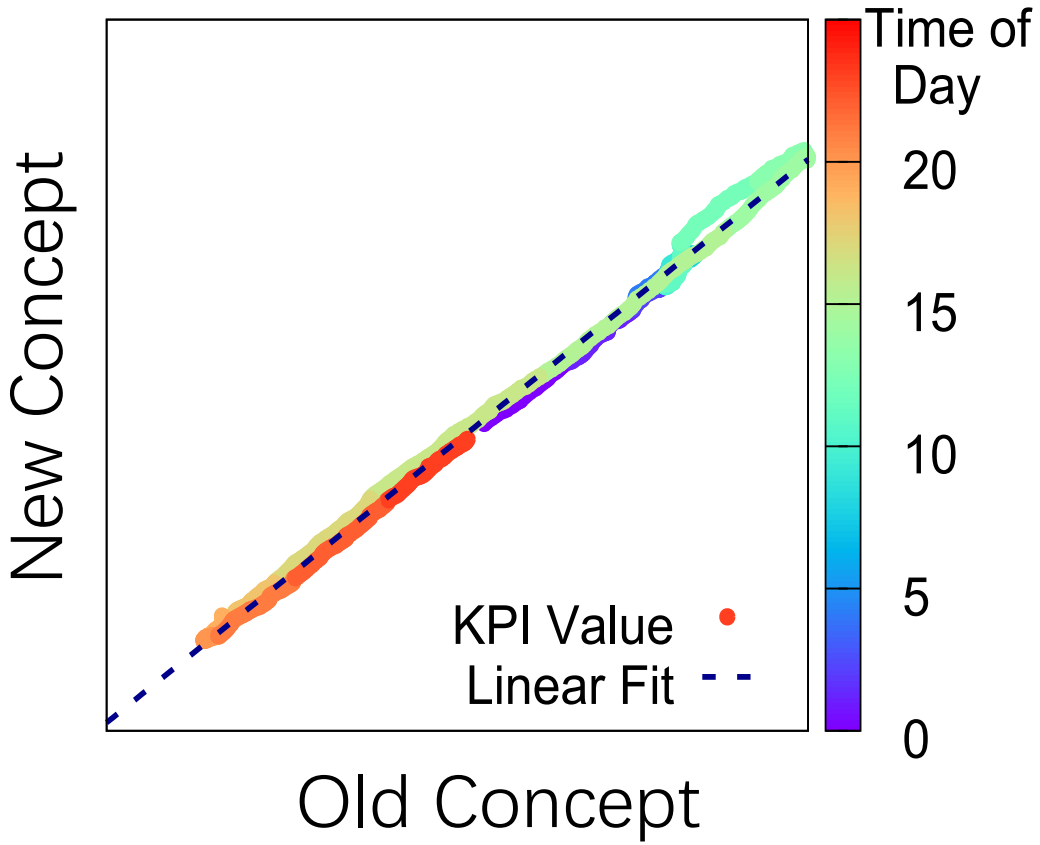
RLM Adaption



Observation: Old and New Concept Can Be Linearly Fitted

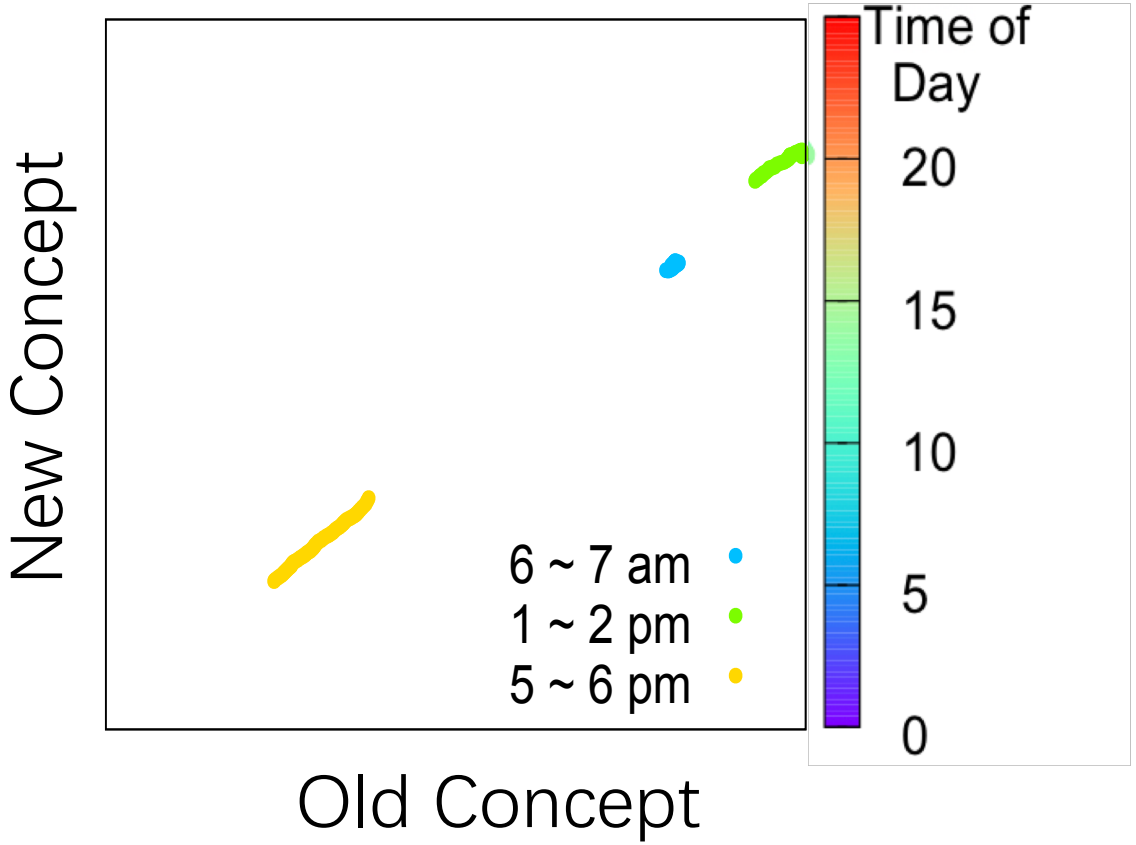


Observation: Old and New Concept Can Be Linearly Fitted



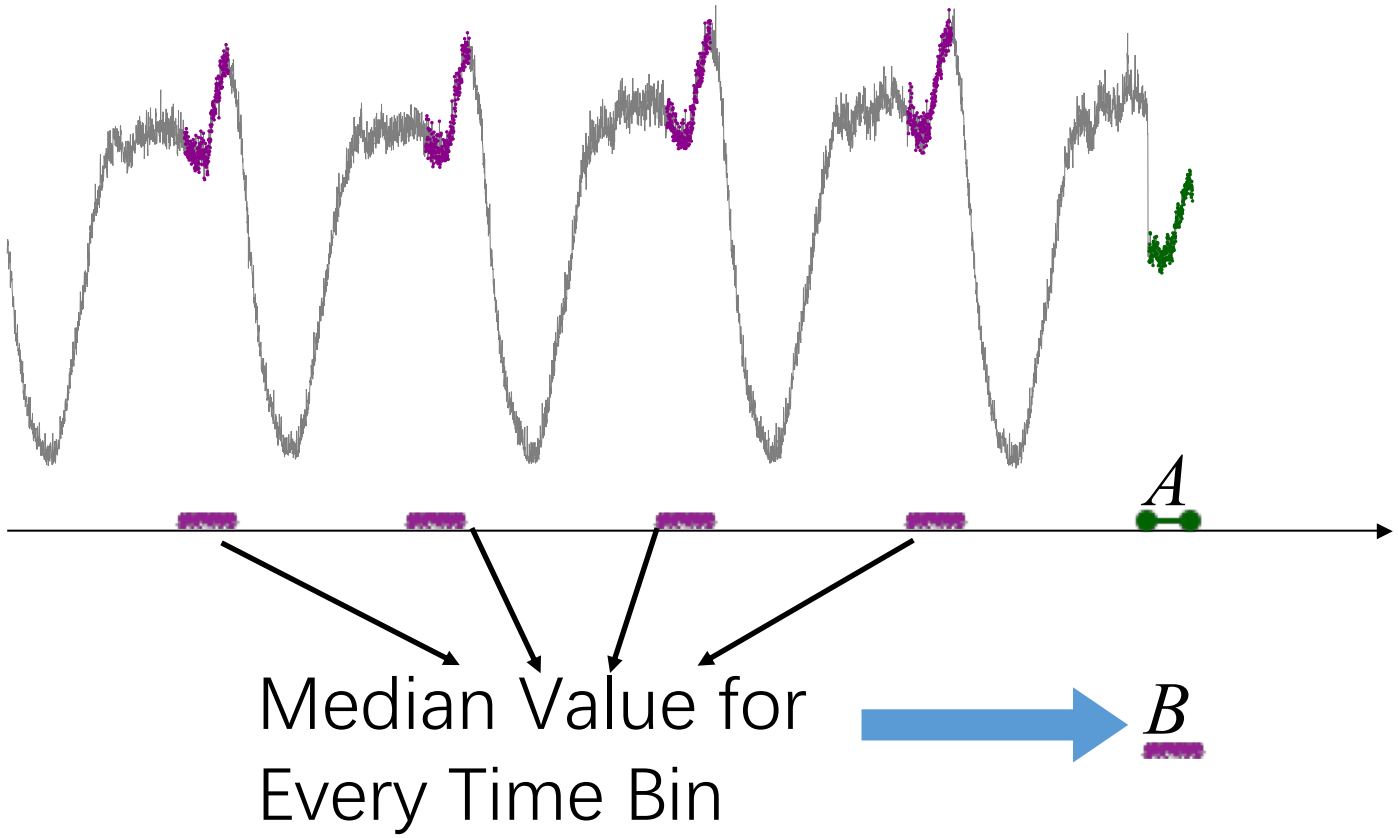
Physical meaning: software on-demand scaling up/down

Challenge: Modeling Linear Relationship in Real-Time



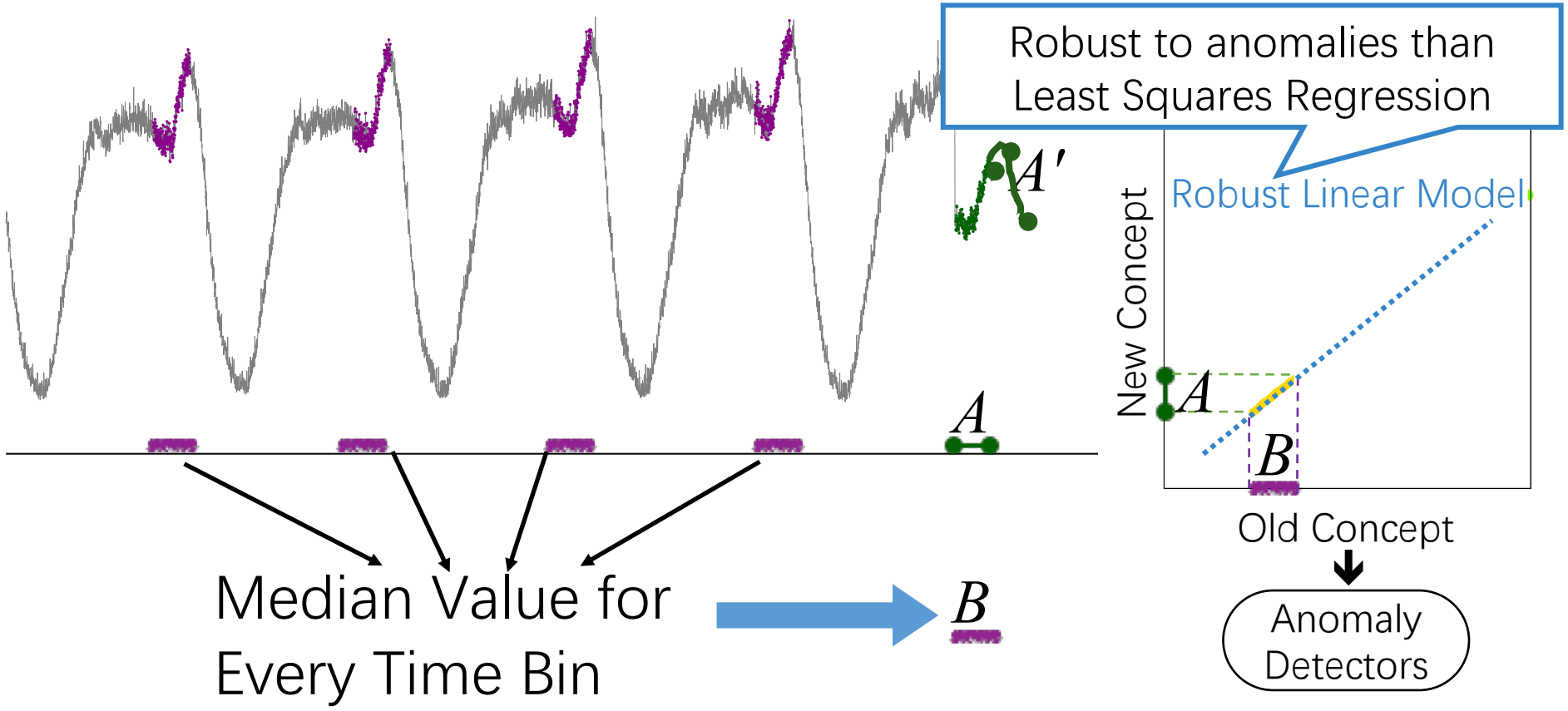
Idea #3. RLM Adaption

Adaption Algorithm Using Robust Linear Model

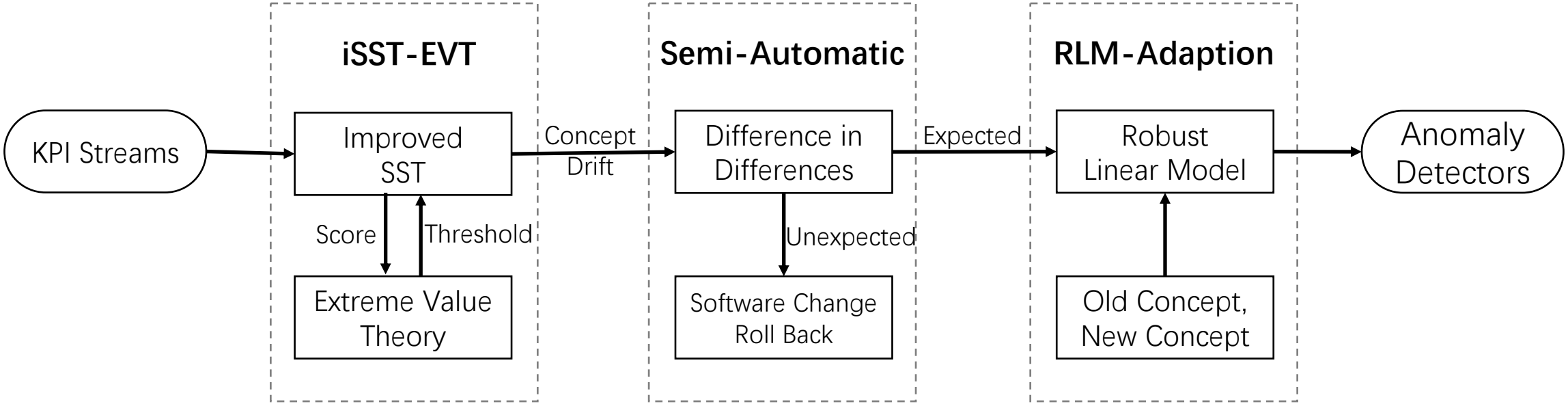


Idea #3. RLM Adaption

Adaption Algorithm Using Robust Linear Model



StepWise Prototype Has Been Deployed in Sogou



Outline

What's concept drift? ➔ KPI distribution change

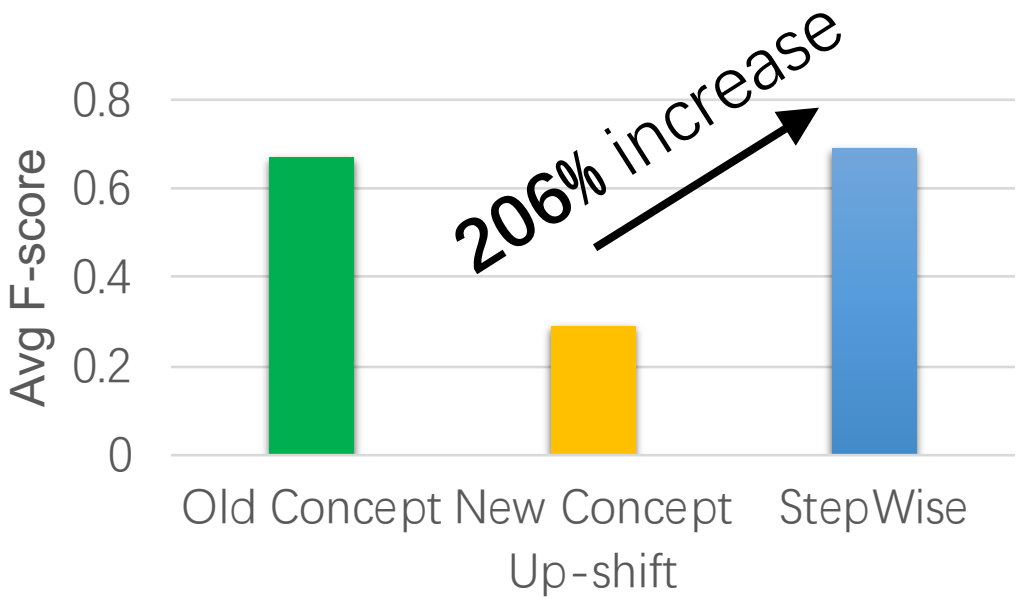
Why it's challenging? ➔ Four challenges

How to adapt to it? ➔ Detection, classification, adaption

Evaluation ➔ 288 labeled KPIs over six months

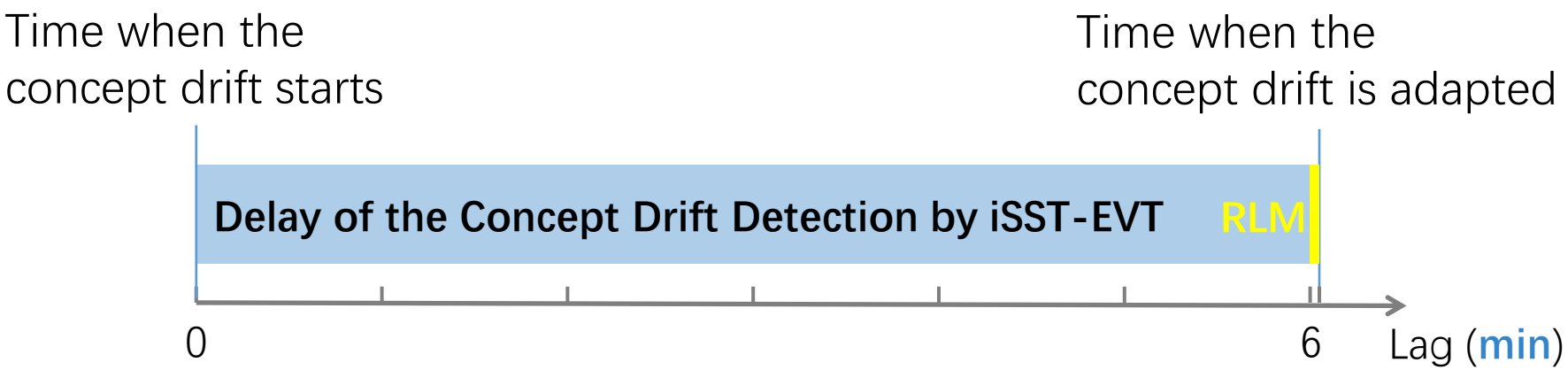
F-score of Anomaly Detection Algorithm

(EWMA, Holt-Winters, TSD etc.)



Substantial accuracy improvement by StepWise

Adaption Lag



Without any adaption, it will take **days** for operators to tune the parameters and thresholds of anomaly detectors

StepWise is rapid enough to adapt to concept drift

Conclusion

- The accuracy of anomaly detection degrades because of the **concept drift**
- Challenges: scalability, robustness, and adaption delay

StepWise uses **domain-specific insights**

- iSST-EVT: no need to tune per-KPI parameter or threshold
- RLM: robust and rapid adaption to diverse types of detectors

Evaluation

- Real world KPI anomalies and concept drifts
- Improve F-score by 206% over a baseline without any concept drift adaption

StepWise
ISSRE 2018

Thank you

mmh16@mails.tsinghua.edu.cn