# Survey on Models and Techniques for Root-Cause Analysis

### 基本信息

##### 作者：

Marc Sol ́e…

##### 研究问题和特点：

* 关注IT系统RCA中用到的模型（model）和模型使用的生成（generation）和推断（inference）算法
* 在性能和可扩展性上对不同需求的的技术进行分析。
* 引导，如何针对于特定的系统选择合适的RCA策略。

##### 文章结构

* Introduction
* 概念和术语介绍
* 主要的models for RCA
* 用于模型的inference algorithm
* 总结

### 重点内容

##### 核心概念

causality（因果关系 ）和 explanation（ 解释，说明，理由，原因，）通常被认为是RCA的输出（output）

##### 术语Terminology

Event: an exceptional condition

Fault/problems/root causes: 是指源头的Events，只有它造成别的event，而非被别event导致。分为三类—permanent/ intermittent(间歇的) /transient

Error：由一个或者多个Fault造成

Failure：从系统外可以观测的Error

Symptom：一个Error的外部表征（manifestation)

Root Cause Analysis：也可以称为fault localization、fault isolation、alarm/event correlation。含义是：the process of inferring the set of faults that generates the given set of synptoms。

##### 系统对于RCA的影响因素

Analysis intent：意图，是需要获得观测到的symptoms的root cause，还是需要解释root cause如何和symptom产生联系。

Analysis time：非功能性需求，即算法能够用来进行推断的最大时间，分为两类场景---real-time diagnosis（响应时间很关键，解决方法是预先计算部分或者全部inference process），post-morten diagnosis（时间限制并不重要）

Complexity：复杂度，包含System Size、Data Size、Inference Length(从symptom到fault被遍历到的最大组件数)、Effect propagation time（一个组件状态的改变需要一定时间才能影响到其他临近组件，有时被忽略或认定为即时的，有时它决定了相关探测的window,决定了Observation Data Size）、Evolution rate（被诊断的系统的变化速度和程度）、Domain knowledge required、System knowledge required（诊断系统对被诊断系统所需要的访问级别）

##### RCA workflow

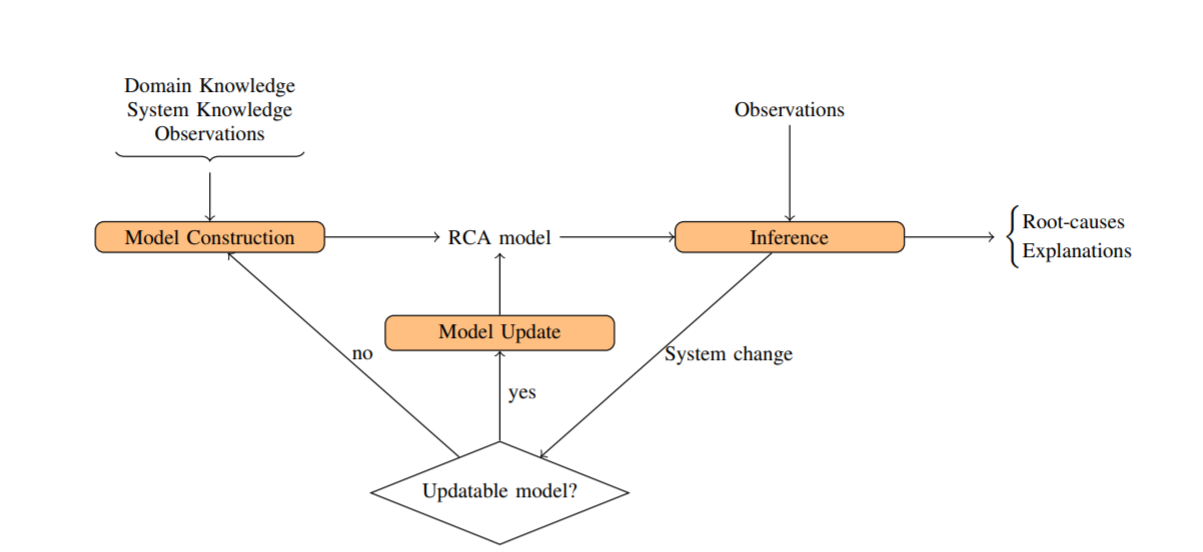


Figure :

##### RCA模型的生成

inference process当中关键的一个特点是：Performance。

许多的推断模型都来自AI，大致分为两大类：

1. Deterministic确定式模型
2. Probabilistic概率式模型

图表简要展示不同类型的RCA模型

…

为什么一些ML中的分类器没有占领RCA领域？

1. 它们通常只返回一个预测的root cause，无法获得解释
2. 很难和domain knowledge结合起来，不能产生逻辑规则
3. 它们往往被简化成了single-label classifier，当需要进行多种故障的检测时，需要和多种classifier协同工作

什么因素对诊断的性能影响最大？

* Size：可以理解为是基本的分析元素的数量，通常是组件component的数目，但是也可以有多个Size属性。
* Inference structure：它定义了不同的elemental analysis element是如何相互关联到一起的。通常利用**Inference Length**指标来进行判别。

##### 如何生成RCA模型？

模型的Size（用来构建系统的基本分析元素的多少，主要取决于系统建模时抽象的层次）和Inference structure（定义不同的基本分析元素是如何相互联系的）对整个模型很重要。

主要有三类方式：

1. Manual generation：专家来提供模型；模型会比较准确，但是知识的elicitation（引用）会很慢且对人来说比较复杂。
2. Assisted generation：根据相当数量的以子模型库的形式出现的domain knowledge 和向下的system information ，产生最后的诊断模型。
3. Automated generation

##### learning model for RCA

当没有domian knowledge和专家手工的一些协助方法可用时，只能采用learning algorithm，学习raw data of the system。

learning algorithm 往往能够学习structure 和 internal parameter。