主动容错技术 FTC：一份技术报告

lpdink*

lpdink@qq.com

Abstract

物理安全通常指保护计算机系统免受硬件设备问题导致的系统故障的安全场景。**容错技术**被广泛应用在系统安全，物理安全，网络安全等多种场景。物理安全场景下的**系统安全**，则主要指硬件设备安全问题。在物理安全场景引入容错技术，可以降低系统组件故障或不稳定性导致的系统性能下降或崩溃的可能。本文选择了容错技术领域最受关注的**主动容错控制系统 (Fault tolerance control system，FTC)**，抽象了面向故障场景的控制系统模型，介绍了 FTC 系统的核心思想及分类，讨论了**故障检测和隔离模块 (Fault detection and isolation，FDI)** 在 FTC 系统中的重要性。

1 简介

在经典控制系统场景下，我们通常假定系统的所有组件都正常且准确地发挥工作。但在实际生产场景下，这种假设显然是与实情不符的：系统组件，尤其是 IOT 系统或分布式系统组件，常常面临着极端天气，网络通信故障，设备断电，损坏，被恶意攻击干扰或侵占等复杂情况。

近些年来，学术界及工业界在这类物理安全场景，引入了容错技术，来提高系统的鲁棒性、健壮性、整体弹性。其中最重要的，也是容错系统核心的，就是容错控制系统 (FTC)。

FTC 技术分为主动和被动方法，本文将专注在主动容错控制上。这项技术最早在工业界生产中使用，1991 年由 Stenge[2] 等人提出最早的综述文章，从概念上明确了 FTC 的基本概念和人工智能技术在 FTC 系统中的应用。1997 年 Patton[3] 回顾了 FTC 技术的发展，并分析了 FTC 系统设计的关键问题。2011 年 Alwi[4] 等人回顾了 FTC 中不同类型的故障，简要概述了故障检测和隔离技术。

此后，在航空航天领域，发动机，光伏通信，电力系统中的 FTC 特化应用也被广泛研究。

*本文是对 <A Survey on Active Fault-Tolerant Control Systems>[1] 的阅读报告.

Using NeurIPS 2022 LaTeX template and style.

但是，此前的研究往往仅将目光放在基于硬件冗余的 FTC 方法上，或是单独地研究故障检测与隔离技术（FDI）并未将两者联合考虑。本篇综述联合考虑了 FTC 和 FDI 技术，将他们统一概述为构成主动 FTC 系统的部分。同时论述了，自从上一综述工作后，主动 FTC 系统领域的最新成果与进展，比较了被动式和主动式 FTC 系统的核心思想。讨论了 FTC 及 FDI 的分类方法，不同种类的系统或模块的核心思想和方法，以促进本领域的进一步研究和发展。

2 问题定义

FTC 系统是在生产实践中被广泛应用的系统，要讨论这样的实例系统，需要首先给出实际系统的概念模型，并确定系统中关键概念的定义。

具体来说，本节讨论故障的定义，分类与原因，并在此基础上，给出 FTC 系统的定义。

2.1 故障定义

故障定义在控制系统中，指会危及系统稳定性并降低系统性能的，与系统标定参数与状态的*偏差*。系统中发生单一故障的影响，从导致性能下降到完全故障（崩溃）不等。

系统故障与外部对系统的干扰不同，如果发生外部干扰，没有破坏系统内在，且系统仍然在符合设计预期地工作，并在干扰消失后，系统将重新回到正常工作状态，这一情况不构成系统故障。故障指系统不符合设计预期的工作状态，属于应该被检测并通过冗余等控制手段，消除影响的元素。

干扰与模型不确定性在实际生产中不可避免地存在并经常出现，他们往往影响着系统的性能，要求系统设计者采用故障控制手段对其进行预期和管理，即系统的鲁棒性设计。而故障是超出系统鲁棒性设计范畴的要素，当故障发生时，系统的鲁棒性控制手段不再能使系统或系统部件正常工作。可见，故障不可恢复，因此需要*冗余设计*。

2.2 故障类型与原因

故障因控制系统的不同组件出错而区分为不同的类型。因此，在讨论故障类型前，先抽象一个简单的现代控制系统的模型。

经典控制系统是一个接收外部命令，包含控制器，执行器，设备，传感器四个组件的闭环系统。控制器接受传感器的回传信息，根据内置逻辑或传入的命令，决定对系统的控制行为，将控制命令发送给执行器。执行器接受控制命令，按照设备 IO 接口的协议，将命令翻译设备能理解的 IO 信号，以控制设备行为。设备接受行为控制命令，并开始进行工作。设备的工作结果将影响整个系统的状态，状态的变化被传感器感知并记录，回传给控制器模块，以决定下一时间步的系统决策。

基于这一现代控制系统的抽象模型，我们可以给出基于组件类型的系统故障分类：

- 设备故障：改变系统的动态 IO 属性，系统很大概率陷入完全不工作状态。

- 传感器故障：执行状态不受影响，但传感器读数存在严重错误，影响控制器决策，系统行为完全不正常。

- 执行器故障：执行状态不受影响，但设备接受的控制信号被中断或篡改。

造成这些故障的原因颇多，包括物理域的剧烈震荡，连接不当，电路短路; 恶意攻击者的虚假信号注入; 机械阻塞; 参数值突变等等。

2.3 FTC 系统的定义

FTC 是自动消弭系统组件中的故障影响，保持系统稳定性及所需的整体性能水平的容错控制系统，旨在提高控制系统对故障场景的安全性和可靠性。基于对故障信息的依赖，FTC 系统可以分为两大类：被动 FTC 和主动 FTC。被动 FTC 不依赖于错误信息来控制系统，与系统鲁棒控制密切相关，其核心在于，使用冗余应对系统的预定义故障。

与被动 FTC 系统相比，主动 FTC 系统基于系统中发生的故障执行。在此类控制系统中，FDI 单元用于查找故障位置并测量其大小；然后，监控控制器决定如何修改控制结构和参数以消弭系统中发生的故障。可能采取的行为包括重新配置，管理冗余，和分析冗余变化。

3 主动 FTC 与 FDI

3.1 主动故障控制 FTC

如上节所述，主动 FTC 使用检测技术来发现故障，然后，监控系统将决定如何修改控制结构和参数以消弭系统中故障的影响，因此主动式 FTC 设计具有三个关键步骤：检测、监督、控制。基于三个关键步骤，主动 FTC 的设计要求：

- **检测高准确性**：FTC 系统本身是用于系统的故障控制，以增强系统鲁棒性的，但由于主动 FTC 有自己额外的控制器，其行为会影响系统的行为。故在主动 FTC 检测单元不准确时，其采取的故障控制行为，反而有可能危及系统的稳定性。因此，主动 FTC 的检测单元被要求具备更高的准确性，并采取保守策略。

- **监督鲁棒性**：故障的发生往往是因为系统遭遇了较大的外部侵害，包括环境和物理侵害，主动 FTC 系统的控制器，被要求在遭遇这些极端状态时仍能正常工作，常见情况是，获得了不弯曲的故障检测信息，以保证其调控冗余，消弭故障的功能正常作用。

- **控制及时性**：故障恢复所花费的时间应该少于恢复的可用时间。换言之，故障弥补行为应该足够迅速，以保证系统稳定性和性能。

基于上述要求，今年来 FTC 对故障弥补的策略，可以分为以下几种：

- **基于开关的** [5]：提供一组预定义的候选控制器，常态情况下，系统在一般控制器的控制下工作，当系统发生故障时，切换到故障控制器下工作。

- **层次结构的**：将 FDI 与 FTC 模块进行了整合，在检测和隔离系统控制后，控制器可以通过自适应策略 [6] 自行重新配置。

- **Safe Parking**[7]：核心思想是，在系统出现故障时，将系统维持在恰当的临时平衡点，保证系统的临时正常工作，防止正反馈循环导致的进一步损害。直到主动控制器将系统调整回标定状态。

- **分析反馈的** [8]：这一方法强烈依赖精确的，延迟极小的 FDI 信息。控制系统在 FDI 与故障控制器之间构成第二个控制闭环，根据 FDI 实时信息，不断调整系统状态，直到到达标定状态。

3.2 故障检测 FDI

如上节所述，主动 FTC 的性能与鲁棒性强烈依赖着 FDI 模块的性能与准确性，因此，具有在线故障检测和隔离能力的准确 FDI 设计是主动 FTC 设计的必要条件。

FDI 模块本质上是一个观察器，用于估计系统的状态和输出，需要综合考虑系统状态，控制输入，输出，量化执行器、设备和传感器故障，未知干扰及不确定性。FDI 根据上一时间步的状态，及本时间步的输入，估计下一时间步的输出，当期望预测与下一时间步的输出偏差过大时，认为系统处于故障状态。

FDI 是一个时序的状态预测器，其采用的方法，通常包括基于模型的 [9]，基于知识的 [10]，和模型-知识的组合方法 [11] 三种。

值得注意的是，在控制领域的模型，指经典的抽象真实问题为数学模型，再加以数学方法的控制；而基于知识的方法，则指利用机器学习（如 SVM）或深度学习方法，采集历史数据，训练模型完成预测。

与人工智能方法的利弊一致，FDI 中基于模型的方法，需要根据特定的场景，决定应用的具体数学模型，需要较强的专家领域知识。而基于知识的方法，则需要大量的历史数据，以训练机器学习或深度学习模型。模型-知识的混合方法则更加灵活，允许 FDI 考虑机器学习模型难以学习到的特定少数情况。

4 结论

本篇综述对主动容错控制系统近些年的成果和进展做以报告，给出了故障的定义，及在故障控制场景下，简单控制模型的抽象。联合分析了 FTC 系统与 FDI 模块，并对 FTC 系统和 FDI 模块的分类做以说明，分析了不同类型系统或模块的主要思想及优缺点，体现了本文的技术报告性质。

References

[1] Alireza Abbaspour, Sohrab Mokhtari, Arman Sargolzaei, and Kang K. Yen. A survey on active fault-tolerant control systems. *Electronics*, 2020.

[2] Robert F. Stengel. Intelligent failure-tolerant control. *IEEE Control Systems Magazine*, 1990.

[3] Ron J. Patton. Fault-tolerant control: The 1997 situation. *IFAC Proceedings Volumes*, 30(18):1029–1051, 1997. IFAC Symposium on Fault Detection, Supervision and Safety for Technical Processes (SAFEPROCESS 97), Kingston upon Hull, UK, 26-28 August 1997.

[4] Halim Alwi, Christopher Edwards, and Chee Pin Tan. Fault detection and fault-tolerant control using sliding modes. 2011.

[5] Lingli Lu, Bin Jiang, and Hao Yang. Supervisory fault tolerant control design for a class of unmanned aerial vehicles. *chinese control and decision conference*, 2011.

[6] Xiaodong Zhang, Marios M. Polycarpou, and Thomas Parisini. Adaptive fault diagnosis and fault-tolerant control of mimo nonlinear uncertain systems. *International Journal of Control*, 2010.

[7] Rahul Gandhi and Prashant Mhaskar. A safe-parking framework for plant-wide fault-tolerant control. *Chemical Engineering Science*, 2009.

[8] Alireza Abbaspour, Kang K. Yen, Parisa Forouzannezhad, and Arman Sargolzaei. An adaptive resilient control approach for pressure control in proton exchange membrane fuel cells. *IEEE Transactions on Industry Applications*, 2019.

[9] Donald L. Simon, Sébastien Borguet, Olivier Léonard, and Xiaodong Zhang. Aircraft engine gas path diagnostic methods: Public benchmarking results. *Journal of Engineering for Gas Turbines and Power-transactions of The Asme*, 2013.

[10] Achmad Widodo and Bo-Suk Yang. Support vector machine in machine condition monitoring and fault diagnosis. *Mechanical Systems and Signal Processing*, 2007.

[11] Heidar Ali Talebi, Khashayar Khorasani, and S. Tafazoli. A recurrent neural-network-based sensor and actuator fault detection and isolation for nonlinear systems with application to the satellite's attitude control subsystem. *IEEE Transactions on Neural Networks*, 2009.