doi: 10.1631/FITEE.1601540

题目：一种非侵入式的基于功耗的可编程逻辑控制器异常检测方案

概要：工业控制系统广泛应用于关键基础设施的建设中，关系到国计民生，因此，攻击者越来越多地将其作为攻击目标，并造成严重的破坏。可编程逻辑控制器（Programmable logic controller, PLC）作为工业控制系统中的核心组件，能够直接控制现场设备，一旦 PLC 中运行了恶意程序，则可能直接造成重大财产损失甚至是人员伤亡。近些年来，针对 PLC 的攻击事件显著增加，这表明 PLC 存在很大的脆弱性，同时也提醒人们保护 PLC 安全的重要性。不幸的是，传统的入侵检测系统和杀毒软件并不能很好地保护 PLC 的安全，因此，针对 PLC 的有效的安全防护方案有待被研究。基于上述背景，本文提出了一种非侵入式的基于功耗的 PLC 异常检测方案。该方案通过分析 PLC 运行时的功耗变化来检测 PLC 中是否运行异常程序，分为功耗信息获取与功耗分析两部分。采集功耗信息是通过在 PLC 的供电线上串入一个电阻实现的，当 PLC 运行时，测量电阻两端的电压即可获取 CPU 的功耗信息。为了更好的分析功耗信息，本文首先从原始功耗数据中提取有效的特征值组合，然后利用正常样本来训练一个基于长短记忆（long short-term memory, LSTM）单元的神经网络模型，利用该模型对后续正常样本进行预测，通过比较测量到的功耗信息与预测的功耗信息，可以确定当前 PLC 中运行的程序是否为正常程序。该方案的优点是无需对原工控系统的封装部分进行软硬件的修改，且无需负样本即可实现对未知攻击的检测。我们在实验室测试平台上对该方法进行了评估，实验表明，对于原程序，只需改动 0.63%即可达到 99.83%的准确率。

关键词：工业控制系统；可编程逻辑控制器；边信道；异常检测；基于长短记忆单元的神经网络模型