Grundlagen

1. Signalakquirierung

Um die Verwaltung von Maschinen innerhalb eines Industriekomplexes zu erleichtern, verwenden Unternehmen heutzutage industrielle Systeme, die zunehmend miteinander verbunden sind und zunehmend drahtlose Kommunikation verwenden. Dank dieser Art von Kommunikation ist es viel einfacher, Informationen über den Zustand und den Betrieb von Maschinen zu sammeln, diese aber auch von einem einzigen Computer aus fernzusteuern. Diese Kommunikation verwenden jedoch einfach und bekannte Protokolle wie das Transmission Control Protocol (TCP). Es ist dann für eine externe Person, die mit diesen Arten von Protokollen vertraut ist, einfach, die Kommunikation innerhalb des Systems zu beobachten und sie zu stören, indem beispielsweise die Kommunikation mit einem Teil des Systems blockiert wird. Ein böswilliger Mitarbeiter kann aber auch aus dem Industriekomplex heraus angreifen, indem er eine Maschine manuell sabotiert oder Malware über einen USB-Stick injiziert.

Cyber-Angriffe dieser Art sind bereits aufgetreten, insbesondere im Jahr 2010 während des Cyber-Angriffs Stuxnet auf Nuklearanlagen im Iran. Malware wurde von einem Mitarbeiter über einen USB-Stick injiziert, um Geräte für die Kernforschung zu zerstören. Der Computerwurm replizierte zunächst selbstständig auf den Maschinen [1] und analysierte die Kommunikation mit SCADA (Supervisory Control and Data Acquisition) und lokalisierte alle Computergeräte unter Verwendung von Windows als Betriebssystem. Windows ist das von Herstellern am häufigsten verwendeten Betriebssystem und ein leichtes Ziel für Angreifer. Durch Ausnutzen eines Fehlers in diesem Betriebssystem konnte der Computerwurm Zugriff auf die Programmlogik-Steuerung (SPS) erhalten. Der Wurm kann daher Codes blockieren, die in die SPS eingegeben werden, und schlechte Informationen an andere Maschinen und IT-Geräte senden. Die Malware könnte auch über USB angeschlossene Geräte infizieren, wodurch sie schnell in den gesamten Industriekomplex eindringen konnte [2].

Ein weiteres neueres Beispiel kam Anfang dieses Jahres mit einem Angriff auf eine Wasseraufbereitungsanlage in den Vereinigten Staaten. Eine Person außerhalb dieser Anlage hat es geschafft, die Kontrolle zu übernehmen, indem sie erneut einen Fehler im Windows-Betriebssystem eines der Computer ausnutzte, der den Gehalt an chemischen Elementen im Wasser verwaltet, und diese Rate auf extrem hohe Werte erhöhte. Hoch, was zu einer Wasservergiftung führte, die gefährlich sein könnte zum Verzehr. Dieses Eindringen konnte jedoch von einem der Mitarbeiter festgestellt werden, der die seltsame Bewegung seines Computerzeigers bemerkte, während sich die Maus nicht bewegte.

Diese industriellen Systeme sind jedoch nicht ohne Verteidigungssystem. Das bekannteste System ist das Network Intrusion Detection System (NIDS). NIDS analysiert eingehende Pakete im Switch und erkennt Kommunikationsstörungen. Das Funktionsprinzip wird in Abbildung 1 dargestellt.

In einem industriellen System übermittelt der Prozess Informationen über den Status seiner Sensoren und Aktoren an den Buskoppler, der die Informationen an speicherprogrammierbare Steuerung (SPS) sendet. Die SPS sendet die Daten an den Switch, der die Daten an eine Firewall und dann an einen Computer zurücksendet.

Während eines Cyberangriffs greift der Computerwurm wie Stuxnet oder Irongate hauptsächlich die SPS an, wodurch der Prozess unterbrochen wird, während schlechte Informationen an den Switch gesendet werden. Daher können die NIDS diese Art von Angriff nicht erkennen, da sie nicht wissen können, dass die SPS gehackt wurde.

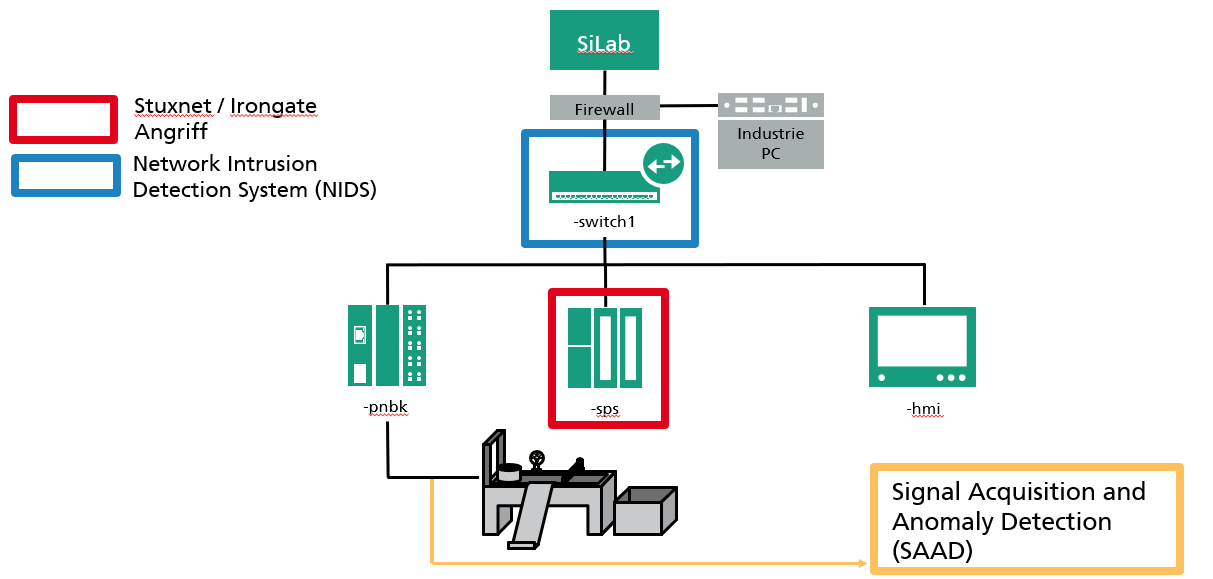


Abbildung 1: Industrielle System Beispiel

NIDS erkennt die Stuxnet- und Irongate-Angriffe jedoch nicht, da diese Angriffe auf der SPS auftreten und sie daher die Kontrolle über den Prozess übernehmen können, während sie dem Switch und anderen Komponenten falsche Informationen über den Status des Prozesses senden.

Um das Verhalten des Prozesses weiterhin kennen zu können, werde ich die analogen Signale der Sensoren und Aktoren direkt am Ausgang des Prozesses analysieren. Diese Signale geben Auskunft über das Verhalten des Prozesses in Echtzeit. Dank meines Systems namens Signal Acquisition and Anomaly Detection (SAAD) erkenne ich eine Anomalie im Verhalten des Prozesses. Auf diese Weise kann ich jede Verhaltensänderung unabhängig vom industriellen System, seinen Komponenten, dem den Prozess steuernden Computer, der Software und dem verwendeten Betriebssystem erkennen.

1. Process

Der Prozess, an dem ich gearbeitet habe, ist eine Maschine von Fraunhofer IOSBs, die Objekte (Bucket) nach ihrer Beschaffenheit sortiert. Das komplette System wird in Abbildung 2 dargestellt.

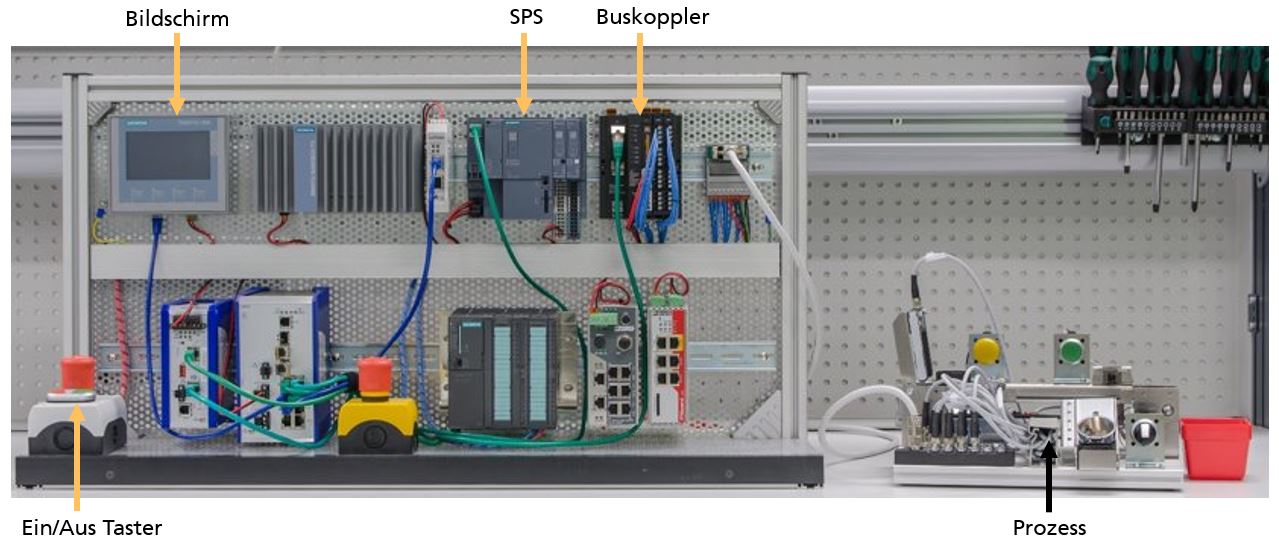


Abbildung 2: Komplete System

Das gesamte System enthält wie zuvor gesehen eine SPS, die über den Buskoppler mit dem Prozess kommuniziert. Die SPS ist mit dem Switch verbunden, der Informationen an den Bildschirm sendet. Der Switch wird auch verwendet, um Angriffe im System zu implementieren.

Der Prozess ist einfach und umfasst verschiedene Elemente: eine Lichtschranke, die erkennt, wann ein Objekt durch sie durchgeht, einen induktiven Sensor, der die Beschaffenheit des Objekts erkennt, ein Laufband, der in beide Richtungen (links oder rechts) gehen kann, eine Taster der das Laufband nach links gehen macht, eine Schranke, eine Ein / Aus-Schalter und eine Lampe, die blinkt, wenn der Prozess eingeschaltet ist, und eingeschaltet bleibt, wenn der Prozess aktiviert wird. Das Funktionsprinzip wird in Abbildung 3 dargestellt.

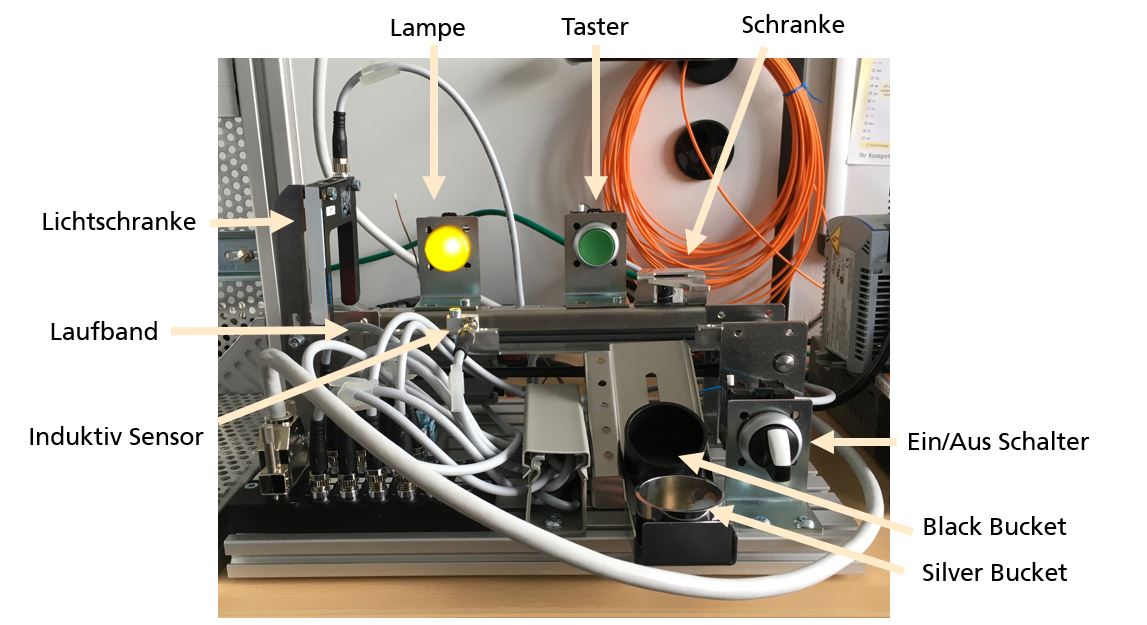


Abbildung 3: Prozess

Der Prozess hat vier normale Verhalten. Der erste ist, wenn der Notfallknopf gedrückt wird, sollte der Prozess beendet werden. Das zweite ist, wenn Sie den Knopf drücken, der das Laufband nach links rollt. Die letzte beide Verhalten treten auf, wenn Sie einen Bucket in der Lichtschranke stecken. Wenn der Bucket silbern ist, rollt das Laufband nach rechts, die Lampe bleibt an, der induktive Sensor erkennt den silbernen Bucket und die Schranke geht runter. Wenn der Bucket schwarz ist, ist das Verhalten dasselbe, außer dass der schwarze Bucket vom induktiven Sensor nicht erkannt wird und daher die Schranke nicht runter geht.

Diesen Verhalten werden von verschiedenen maschinellen Lernen Methoden gelernt. Damit können wir eine Anomalie mit Vergleichung des Outputs die Methoden erkennen.