Grundlagen

1. Signalakquirierung

De nos jours, pour faciliter la gestion des machines au sein d’un complexe industrielle, les entreprises utilisent des systèmes industriels qui sont de plus en plus connectées et utilisent de plus en plus les connexions sans fils. Grâce à ce genre de connexions, il est beaucoup plus facile de récolter des informations sur l’état et le fonctionnement des machines mais aussi de pouvoir les opérer à distance à partir d’un simple ordinateur. Cependant, ces connexions utilisent des protocoles de communication basiques et connus telle que le Transmission Control Protocol(TCP). Il est alors facile pour une personne extérieure, connaissant ce genre de protocoles, d’observer les communications au sein du système et de pouvoir le perturber en bloquant les communications vers un élément du système, par exemple. Mais un employé malintentionné peut aussi attaquer depuis l’intérieur du complexe industrielle en sabotant manuellement une machine ou en injectant un malware via une clé USB.

Des cyber-attaques de ce genre se sont déjà passées, notamment en 2010 lors de la cyber-attaque, nommée Stuxnet, sur des installations nucléaires en Iran. Un malware a été injecté via une clé USB par un employé dans le but de détruire des équipements servant à la recherche sur le nucléaire. Le ver informatique s’est tout d’abord répliqué tout seul dans les machines [1] et a analysé les communications vers le Supervisory Control and Data Acquisition (SCADA), et repéré tous les équipements informatiques utilisant Windows comme système d’exploitation. Windows étant le système d’exploitation le plus utilisé par les industriels, il est une cible facile pour les attaquants. En exploitant une faille dans ce système d’exploitation, le ver informatique a pu avoir accès au Program Logic Controller (PLC). Le ver peut dès lors bloquer les codes entrant dans le PLC et peut envoyer de mauvaises informations vers d’autres machines et équipements informatiques. Le malware pouvait aussi infecter les équipements connectés par USB ce qui lui permis de rapidement envahir tout le complexe industriel [2].

Un autre exemple plus récent fût plus tôt cette année avec une attaque sur une centrale d’assainissement d’eau aux Etats-Unis. Une personne extérieure à cette centrale a réussi à prendre le contrôle en exploitant là aussi une faille dans le système d’exploitation Windows d’un des ordinateurs gérant le taux d’élément chimique dans l’eau et a augmenté ce taux à des niveaux extrêmement élevés entraînant un empoisonnement de l’eau pouvant être dangereux à la consommation. Cette intrusion a cependant pu être détecté par l’un des employés remarquant l’étrange mouvement de son pointeur d’ordinateur alors que la souris ne bougeait pas.

Ces systèmes industriels ne sont cependant pas démunis de système défense. Le système le plus connu est le Network Intrusion Detection System (NIDS). NIDS analyse les paquets entrants dans le switch est va détecter les intrusions dans les communications. Das Funktionsprinzip wird in Abbildung 1 dargestellt.

Dans un système industriel, le processus communique les informations sur l’état de ses sensors et actuators au Buskoppler qui envoie les informations au (SPS). Le SPS envoie les données au switch qui s’occupe de renvoyer les données vers un firewall puis un ordinateur.

Lors d’une cyber-attaque, le ver informatique tel que le Stuxnet ou Irongate vont principalement s’attaquer au SPS qui va perturber le processus tout en envoyant de mauvaises informations au switch. Par conséquent le NIDS ne peut pas détecter ce genre d’attaque car il ne peut pas savoir que le SPS a été hacké.

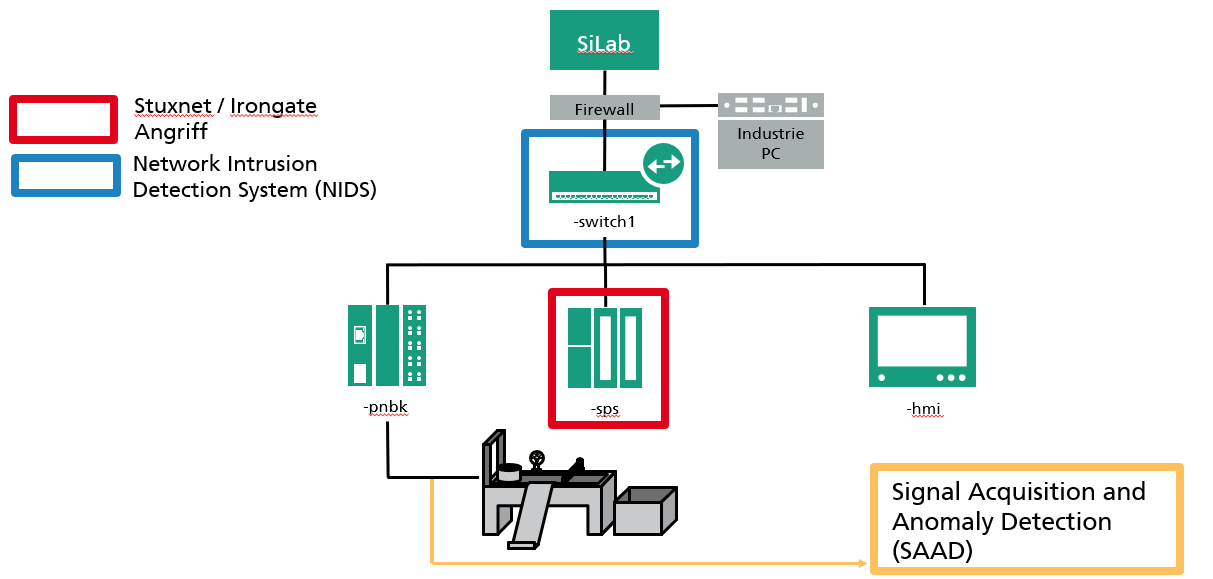


Abbildung 1: Industrielle System Beispiel

Pour pouvoir continuer de connaître le comportement du processus, je vais analyser les signaux analogiques des sensors et actuators directement en sorti du processus. Ces signaux nous indiquent le comportement du processus en temps-réel et grâce mon système appelé Signal Acquisition and Anomaly Detection (SAAD), je détecte une anomalie dans le comportement du processus. De cette manière, je peux détecter tout changement de comportement indépendamment du système industriel, de ses composants, de l’ordinateur contrôlant le processus, du logiciel et du système exploitation utilisée

1. Process

Le processus sur lequel j’ai travaillé est une machine provenant de Fraunhofer IOSBs qui trie des objets (bucket) d’après leur matériau. Das komplete System wird in Abbildung 2 dargestellt.

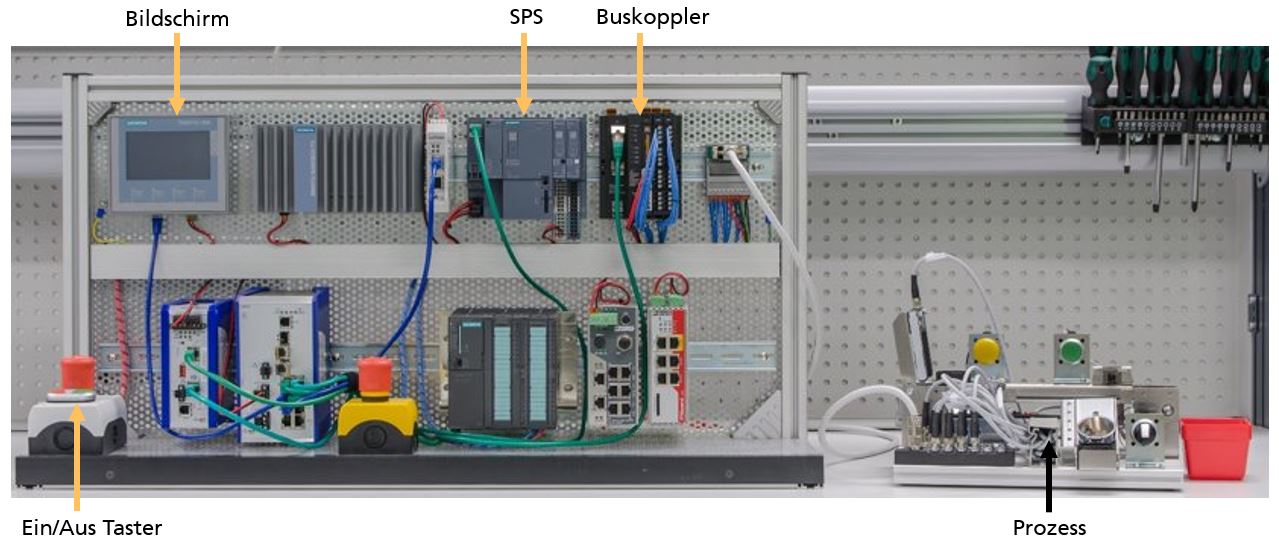


Abbildung 2: Komplete System

Le système entier contient comme vu précédemment un SPS qui communique au processus via le Buskoppler. Le SPS est relié au switch qui envoie des informations à l’écran. Le switch me servira aussi à implanter des attaques dans le système.

Le processus est assez simple et comprend divers éléments : une porte qui détecte lorsqu’un objet la traverse, un détecteur inductif qui va détecter la matière de l’objet, un tapis défilant pouvant aller dans les deux directions (gauche ou droite), un bouton faisant le tapis aller à gauche, un Schranke, un bouton On/Off et une lampe qui clignote quand le processus est allumé et resté allumé quand le processus est activé. Das Funktionsprinzip wird in Abbildung 3 dargestellt.

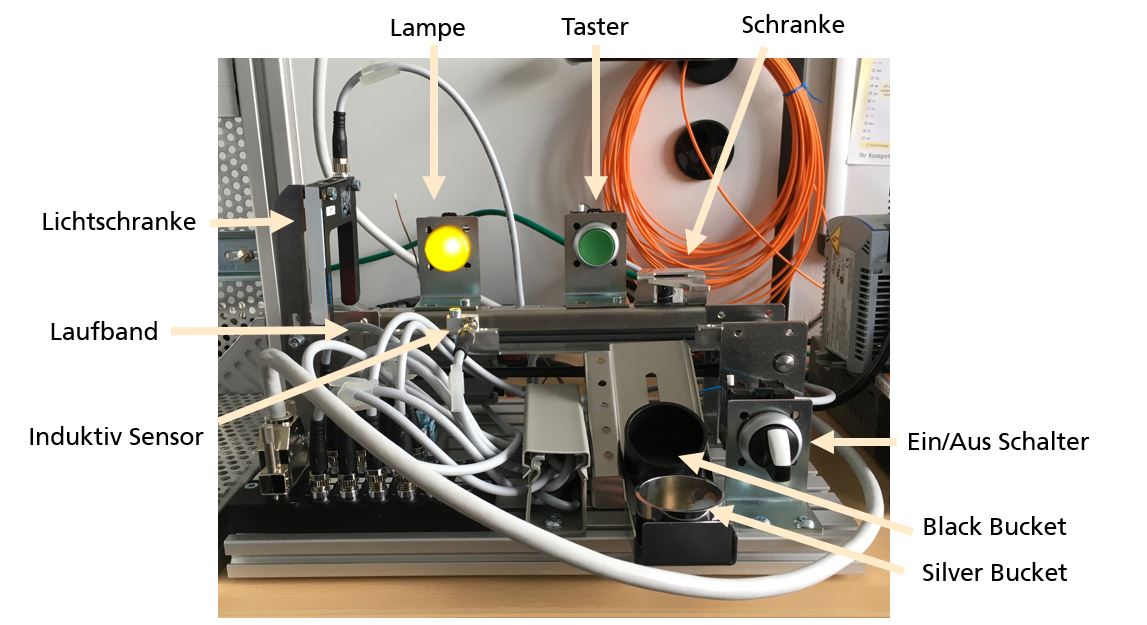


Abbildung 3: Prozess

Le processus a quatres comportements normaux. Le premier est lorsque l’on appuie sur le bouton d’urgence alors le processus doit s’éteindre. Le deuxième est lorsque l’on appuie sur le bouton qui fait défiler le tapis vers la gauche. Les deux derniers comportements sont lorsque l’on introduit un Bucket dans la porte. Si le Bucket est silver, le tapis défile vers la droite, la lampe reste allumée, l’inductif sensor détecte le silver bucket et le schranke descend. Si le bucket est black, le comportement est le même à la différence que le black bucket n’est pas détecté par l’inductif sensor et donc le schranke ne descend pas.

[1] W. Broad, J. Markoff, and D. Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay," New York Times, 15 Jan 11.

[2] D. Kushner, "The Real Story of Stuxnet," IEEE Spectrum 53, No. 3, 48 (2013).