Estimating the Impact of IT Security Incidents in Digitized Production Environments

ABSTRACT

Owing to digitalization, manufacturing companies increasingly integrate IT services – such as control systems – into their production environments. This increases the flexibility of production and allows them to offer new data-based services (e.g., predictive maintenance). However, stepping up production-IT system connections also leads to an increased reliance on the availability of IT services as a means to value creation, both in internal production processes and at the customer interface. More interconnectivity also increases network complexity, and thus favors the rapid spread of cyber-attacks within the information network. The potential for damage is massive, as disruptions to IT services can harm the deliverability of both, connected IT services and production components. Despite existing studies on IT security, little has been written on ways to estimate the impact that *availability incidents* have on digitized production environments based on the IIoT – for example, smart factories. To help close this research gap, we provide an approach that enables users to simulate cyber-attacks and measure the impact of such attacks on value creation in digitized production environments. We compare the features of our model with our specific design objectives and competing artifacts, present our prototype and the results of a sensitivity analysis for selected model parameters, and illustrate the applicability of our model using the real-life case of a German manufacturing company. Our results indicate that the degree of interconnection in digitized production environments is the most important influencing factor when estimating the impact of an IT availability incident on value creation.

Keywords: IT security, cyber attacks, Bayesian Networks, value creation