Zusammenfassung der Dissertation:

Methodik zur Dokumentation und Analyse von Kommunikationsschwachstellen in sicherheitskritischen Systemen anhand von hierarchischen Aufgabenmodellen

von Tomasz Mistrzyk

Die vorliegende Dissertation beschreibt eine Methodik für die Dokumentation und Analyse von Schwachstellen in sicherheitskritischen Systemen. Die Methodik basiert auf einem Kommunikationsmodell und nutzt die Vorteile der systematischen Präsentation von Aufgabenabhängigkeiten in hierarchischen Aufgabenmodellen.

Kommunikation belegt eine Schlüsselposition in sicherheitskritischen Systemen, da sie verantwortlich für die angemessene Koordination von Aufgaben ist. Schwächen innerhalb der Kommunikation der Akteure in sozio-technischen sicherheitskritischen Systemen untereinander werden als Hauptursache für kritische Ereignisse betrachtet. Diese Systeme beinhalten menschliche Akteure, die Aufgaben ausführen und die technischen Geräte, welche die Arbeit der menschlichen Akteure unterstützen.

Das Ziel der Abhandlung ist es, einen systematischen Ansatz zur Dokumentation und Analyse der Kommunikation zwischen Akteuren in sozio-technischen sicherheitskritischen Systemen zu erarbeiten. Um dies zu erreichen, wird ein geeigneter Beschreibungskalkül zur Modellierung der Kommunikation kreiert. Darüber hinaus werden Parameter definiert und ein Vorgehen vorgeschlagen, um die Kritikalität der Schwachstellen in der Kommunikation quantitativ wie qualitativ abzuschätzen und latente Kommunikationsfehler aufzuzeigen.

Der präsentierte Ansatz erlaubt einem Experten, systematisch die Kommunikationsdefizite mit deren Konsequenzen für das System zu identifizieren und zu dokumentieren. Die Methodik wurde mit Hilfe von Fallstudien validiert.