Das Zielobjekt dieser Thesis ist eine Automatisierungsanlage, für diese soll ein Sicherheitskonzept zur Authentifizierung und Autorisierung von Fernzugriffen erstellt werden.

Eine Automatisierungsanlage besteht aus einer Reihe von Sensoren und Aktoren, die zentral und/oder dezentral automatisiert gesteuert werden. Die Automatisierungsanlage, die in dieser Thesis betrachtet wird, ist eine Kälteanlage für Supermärkte mit Steuerungstechnik der Eckelmann AG. Für die Steuerungstechnik der Anlagen gibt es mehrere beteiligte Parteien. Den Hersteller, den Besitzer sowie die Kältetechnikunternehmen. Besitzer spielen im Verlauf dieser Thesis lediglich eine untergeordnete Rolle, da diese meist die komplette Verantwortung an der Anlagen an die Kältetechnikunternehmen abgeben. Der Hersteller liefert die gesamte Technik, welche die Automatisierung und Überwachung der Anlage ermöglicht. Die Kältetechnikunternehmen sorgen für die Inbetriebnahme der Kälteanlage, führen regelmäßige Wartungsarbeiten durch und Überwachen die Funktionstüchtigkeit. Der wichtigste Aspekt für die Thesis ist die Überwachung, welche in Fernservice-Zentralen der Kältetechnikunternehmen stattfindet. Dazu wird ein Fernzugriff auf die Kälteanlage zwingend benötigt. Der Fernzugriff ist eine kostengünstige Möglichkeit für die Kältetechnikunternehmen, viele Kälteanlagen zentral zu überwachen. Durch die Fernwartung ist es auch möglich, regulierend in das Ökosystem einer Kälteanlage einzugreifen, deswegen spielt der Aspekt der Nachvollziehbarkeit eine große Rolle für diese Unternehmen. Nachvollziehbarkeit wird durch Sicherheitsmaßnahmen erreicht, genauer durch Authentifizierung, Autorisierung und Auditing. Unter dem Schlagwort Industrie 4.0 werden immer mehr Firmen darauf aufmerksam, dass durch die zunehmende Vernetzung von Automatisierungsanlagen Sicherheitsrisiken durch Angreifer entstehen, welche das System aus der Ferne kompromittieren können. Durch die Anwendungsintegration zwischen Kälteanlage und Fernservice-Zentrale werden die Daten auch für Angreifer immer einfacher zugreifbar. Dies liegt auch daran, dass die proprietären Datenformate des Herstellers, die zwischen den Komponenten der Steuerungstechnik genutzt werden, für die Fernservice-Zentralen interpretiert und in menschenlesbare Formate gepackt werden. Um Maßnahmen gegen Angreifer umzusetzen, muss zunächst ein Überblick der möglichen Gefährdungen geschaffen werden. Aus diesem Grund werden Sicherheitskonzepte erstellt. Ein Entwurf eines solchen Sicherheitskonzeptes, mit Fokus auf Authentifizierung und Autorisierung, ist der Hauptbestandteil dieser Thesis.

Durch die Bedrohungsanalysen in den Kapiteln 3 und 4 wurden viele Gefährdungen des aktuellen Systems und des Konzeptes für die prototypische Implementierung gefunden. Einen starken Einfluss hierauf hatten die Sicherheitskataloge des Bundesamtes für Sicherheit in der Informationstechnik. Durch die Kataloge konnte auf eine breite Basis von möglichen Gefährdungen zurückgegriffen werden. Anhand der gefundenen Gefährdungen wurden viele Maßnahmen formuliert, die in die Anforderungen der prototypischen Implementierung eingeflossen sind. Für den Benutzerlogin wurde eine Two-Factor-Authentication etabliert. Die erste Authentifizierung findet durch Client-Zertifikate statt, wodurch diese für den Benutzer fast transparent abläuft. Gleichzeitig wird möglichen Angreifern dadurch ein großes Hindernis in den Weg gestellt. Der Einsatz eines Reverse Proxy Servers verhindert zudem, dass DoS-Attacken die Steuerungstechnik der Kälteanlage überlasten können. Für die zweite Authentifizierung des Benutzers werden dessen Benutzername und Passwort benötigt. Diese Daten liegen bereits in den Benutzerverwaltungen der Fernservice-Zentralen vor, deshalb wurde mit dem FreeRADIUS-Server ein Authentifizierungsserver aufgesetzt, der als Multiplexer für alle gängigen Benutzerverwaltungen eingesetzt werden kann.