**Dokumentation: Risikoanalyse**

Im Rahmen der Planung unseres Projekts haben wir eine Risikoanalyse durchgeführt, um potenzielle Gefahren frühzeitig zu identifizieren und geeignete Gegenmaßnahmen festzulegen. Ziel ist es, die Zuverlässigkeit, Sicherheit und Qualität des Systems über den gesamten Projektverlauf hinweg zu sichern.

**Vorgehensweise**

Wir haben zunächst mögliche Standardrisiken gesammelt, die typischerweise bei der Entwicklung eines cyberphysischen Systems auftreten können. Für jedes Risiko wurden folgende Punkte bewertet:

* Wahrscheinlichkeit des Eintretens (z. B. niedrig, mittel, hoch)
* Auswirkungen, wenn das Risiko eintritt
* Eine Ampelfarbe (grün, gelb, rot) zur visuellen Risikobewertung
* Ursachenanalyse zur besseren Nachvollziehbarkeit
* Konkrete Maßnahmen zur Behandlung und Kontrolle

Diese Einschätzung hilft uns dabei, die Priorität einzelner Risiken zu erkennen und frühzeitig geeignete Vorkehrungen zu treffen.

**Ergebnisse**

Insgesamt wurden neun Risiken dokumentiert. Besonders kritisch (Ampelstufe 4) sind:

* **Hardwarekomponenten fallen aus**
* **Unzureichende Testabdeckung**

Diese Risiken wurden als besonders gefährlich eingeschätzt, da sie eine direkte Auswirkung auf die Funktionsfähigkeit oder Qualität des Gesamtsystems haben können. Entsprechend wurden dafür konkrete Gegenmaßnahmen eingeplant, wie z. B. ein stabiles IP-Konzept, Fehleranzeigen und strukturierte Testpläne.

**Ziel der Maßnahmen**

Die in der Analyse dokumentierten Risiken wurden jeweils mit konkreten Behandlungs- und Kontrollmaßnahmen versehen, um entweder

* das Auftreten zu verhindern (präventiv),
* oder die Auswirkungen zu minimieren, falls das Risiko dennoch eintritt (reaktiv).

**Erläuterung ausgewählter Maßnahmen**

* Sensoren liefern fehlerhafte Werte:  
  Um fehlerhafte Alarme oder das Ausbleiben kritischer Warnungen zu vermeiden, werden die Sensoren vorab getestet und kalibriert. Zusätzlich werden regelmäßige Funktionstests im Betrieb vorgesehen, um Abweichungen frühzeitig zu erkennen.
* Verbindungsprobleme zum Interface:  
  Die Verbindung ist zentral für Steuerung und Datenanzeige. Durch ein statisches IP-Konzept und die Integration von Fehlermeldungen im Interface wird sichergestellt, dass Verbindungsprobleme schnell erkennbar und behebbar sind.
* RFID-Zugänge funktionieren nicht:  
  Um ungewollte Zugangsprobleme oder unberechtigten Zutritt zu vermeiden, werden Test-User eingerichtet, ein Protokollierungssystem integriert und die Zuordnung der RFID-Tags regelmäßig überprüft.
* Alarm wird zu spät ausgelöst:  
  Die Verarbeitungskette wird so optimiert, dass eine Echtzeitverarbeitung sichergestellt ist. Schwellenwerte und Parameter werden getestet und bei Bedarf angepasst, um Verzögerungen zu minimieren.
* Fehlende Redundanz im System:  
  Um bei Ausfall einzelner Komponenten handlungsfähig zu bleiben, wird ein Notfallkonzept mit Backup-Komponenten (z. B. Bewegungssensor) eingeplant.
* Sicherheitslücke im Webinterface:  
  Zur Vermeidung unbefugter Zugriffe werden grundlegende Sicherheitsmaßnahmen wie HTTPS-Verschlüsselung, Passwortschutz eingeführt.
* Fehlende Benutzerrechteverwaltung:  
  Ein Rollenmodell (z. B. Admin vs. User) stellt sicher, dass nicht alle Nutzer dieselben Rechte haben. Das Interface wird zudem so abgesichert, dass unautorisierte Änderungen unterbunden werden.
* Hardwarekomponenten fallen aus:  
  Um Ausfälle einzelner Module (z. B. Sensoren, RFID-Leser) zu kompensieren, wird auf modulare Bauweise gesetzt und es werden alle Komponenten ausführlich getestet und als Backup noch Ersatzkomponenten angeschafft.
* Unzureichende Testabdeckung:  
  Dieses Risiko stellt eine ernsthafte Gefahr für die Qualitätssicherung dar. Durch das planvolle Aufstellen von Testszenarien und das Führen von Testprotokollen wird sichergestellt, dass alle Funktionen überprüft werden. So lassen sich Fehler bereits in der Entwicklungsphase erkennen.