Checkliste für Wasserkraftwerke (WKW)

Die 10 Fragen zur IT-Sicherheit

Version: 1.0

Veröffentlichungsdatum: 31.07.2025

Landesamt für Sicherheit in der Informationstechnik, Keßlerstraße 1, 90489 Nürnberg
beratung-kritis@lsi.bayern.de, Telefon: 0911 21549-525

Checkliste für Wasserkraftwerke (WKW) - Die 10 Fragen zur IT-Sicherheit

Die Relevanz einer abgesicherten IT-Landschaft nimmt mit jedem Tag und jeder potenziellen Gefährdung zu. Mit dieser Checkliste soll es auf unkomplizierte Weise ermöglicht werden, den derzeitigen Stand Ihrer existierenden Sicherheitsmaßnahmen grundlegend zu evaluieren. Hierdurch sollen mögliche Optimierungsmöglichkeiten aufgezeigt werden. Diese Checkliste wurde für kleinere und mittelgroße Wasserkraftwerke entworfen und dient der Selbsteinschätzung und Kontrolle der bislang implementierten Maßnahmen.

Im ersten Abschnitt wird mittels der 10 „Fragen zur Selbstkontrolle“ eine erste Beurteilung zum Stand Ihrer IT-Sicherheit vorgenommen. Im Anhang werden die einzelnen Themenbereiche detailliert vorgestellt sowie Maßnahmen und Empfehlungen für den Fall, dass „Nein“ ausgewählt wurde. Abschließend bietet das Glossar einen Überblick über die in der Checkliste und im Anhang verwendete Fachbegriffe und ihre Definitionen. Fachbegriffe, die im Glossar erläutert werden, sind mit * gekennzeichnet.

Das LSI berät gerne zu den nachfolgenden Punkten per Mail an beratung-kritis@lsi.bayern.de oder telefonisch unter der Telefonnummer 0911 21549-525.

Fragen zur Selbstkontrolle	ja	nein	nicht relevant	Anhang
Sind alle wichtigen Unterlagen des WKW vorhanden und sicher aufbewahrt?	☐	☐	☐	1
Sind alle Bauteile des WKW gegen Einwirkungen von außen geschützt?	☐	☐	☐	2
Gibt es eine Sicherung (Backup) von Steuerung, Dokumenten und Konfigurationen?	☐	☐	☐	3
Gibt es einen Wiederanlaufplan falls es zu einem kompletten Ausfall kommt?	☐	☐	☐	3
Werden Störungen der Anlage automatisch an den Betreiber gemeldet?	☐	☐	☐	3
Sind elektronische Steuerungssysteme (z.B. SPS oder PCs) vom Internet getrennt?	☐	☐	☐	4
Sind *Fernzugänge** mit Multi-Faktor-Authentifizierung geschützt?	☐	☐	☐	5
Ist die Anlage vor Manipulationen geschützt, sind die Mitarbeiter ausreichend geschult?	☐	☐	☐	6
Sind auf allen IT-Bauteilen die aktuellen Updates installiert?	☐	☐	☐	7
Werden IT-Bauteile regelmäßig geprüft und kontrolliert?	☐	☐	☐	8

Anhang

Kategorisierung

Die nachfolgende Kategorisierung dienen der Selbsteinordnung und Prüfung, welche der folgenden Aspekte relevant für die Anlage sind.

Kategorie 1:
Es sind keine elektronischen Steuerungssysteme (z.B. SPS oder PCs) vorhanden bzw. verbaut.

Kategorie 2:
Es sind elektronische Steuerungssysteme (z.B. SPS) und Regelungstechnik vom Netzbetreiber (z.B. Rundsteuertechnik) vorhanden (zur Leistungsreduzierung der Anlage, typische Regelstufen beispielsweise 0 %, 30 %, 60 % und 100 %).

Kategorie 3:
Direktvermarkter / Fernwartungszugang / Fernwirkzugang vorhanden (neben dem Netzbetreiber existiert eine weitere steuernde Instanz und/oder es ist ein Fernwartungszugang eingerichtet). Hierzu zählt die Anlage auch, wenn beispielsweise Leistungsdaten etc. auf einer Website abgerufen werden können.

Kategorie 4:
Es ist zusätzlich Leittechnik vorhanden / übergeordnete Steuerung (SCADA).

1. Dokumentation

Kategorie: 1 – 4

Fehlende und mangelhafte Dokumentationen können den Betrieb beeinträchtigen bzw. die Wiederaufnahme des Betriebs nach einer Störung eines WKW erheblich verzögern. Eine sorgfältige Dokumentation ist daher essenziell, um beispielsweise rasch auf mögliche Störungen reagieren zu können.

Sie erleichtert zudem:

- zukünftige Erweiterungen einer bestehenden Infrastruktur,
- die Übergabe an einen neuen Betreiber oder,
- einen Systemwechsel, beispielsweise bei Reparatur oder Modernisierung.

Sind folgende Unterlagen zu dem WKW vorhanden und auf dem neuesten Stand?

- Stromlaufplan / Netzwerkplan mit folgenden Punkten:
    i. Fernzugänge
    ii. Rundsteuerempfänger
- Wasserrechtliche Genehmigungen / Verträge mit Dritten (z.B. Lieferverträge)
- Konfigurationen aller verbauten Technik (z.B. Firewall-Konfigurationen)
- Bedien- und Wartungsanleitung

Existiert ein sicherer, räumlich getrennten Lagerort für essenzielle Komponenten und Dokumente?

Erstellen Sie ein individuelles Backup-Konzept, das auf Ihre Bedürfnisse zugeschnitten ist.

2. Schutz vor physischen Schäden

Kategorie: 2 - 4

Sind die Steuerungssysteme vor folgenden Gefahren geschützt?

- Feuer
- Wasser
- Überspannung
- Stromausfall

3. Backup / Ausfallsicherheit / Systemverfügbarkeit

Kategorie: 2 - 4

Um einen Verlust der Daten bei einem Ausfall zu verhindern, ist es unerlässlich, geeignete Vorkehrungen für eine Systemwiederherstellung zu ergreifen und die Daten bei Änderungen zu sichern.

Die *3-2-1-Backup-Regel* hat sich als besonders effektiv erwiesen. Dabei werden drei Datenkopien auf mindestens zwei unterschiedlichen Medien gespeichert. Mindestens eine Sicherung sollte nach Erstellung vom Netz getrennt aufbewahrt werden. Zusätzlich zu den regelmäßigen Backups empfiehlt es sich eine weitere Sicherung bei der Einrichtung sowie bei Änderungen am System zu erstellen (dabei ist auf jeweilige Vollständigkeit zu achten z.B. von SPS-Programm(en), Konfigurationen und Prozessvariablen).

Weitere Maßnahmen zur Gewährleistung der Ausfallsicherheit und Systemverfügbarkeit:

- (Regelmäßige) Datensicherungen, Konfigurationen (inkl. SPS), Steuerungsprogramme, usw.
- Sichere Aufbewahrung der Backups vor physischen Einflüssen (vgl. Punkt 2 → Schutz vor physischen Schäden) und an verschiedenen Standorten
- Vorhalten baugleicher und bereits eingerichteter Leittechnik-Komponenten (Bauteile können so einfach ausgetauscht werden)
- Automatische Meldung von Störungen an den Betreiber
- Möglichkeit der Bedienung vor Ort als Rückfalloption
- Prüfung, ob ein Wiederanlaufplan notwendig ist (Anlaufschema)

4. Netztrennung

Kategorie: 3 - 4

Grundsätzlich sollte ein Zugriff auf das Leittechniknetz aus anderen Netzwerkbereichen nicht stattfinden. Ein strikt isolierter Betrieb des Leittechniknetzes, d.h. physikalische Leitungstrennung und damit keinerlei Netzübergänge zu allen anderen Netzbereichen des Unternehmens und dem Internet, ist anzustreben. Sollten Netzübergänge benötigt werden, sind diese so zu gestalten, dass die Wahrscheinlichkeit, Opfer eines Cyberangriffs zu werden, so gering wie möglich gehalten wird.

- Steuerungssysteme sind über eine Firewall vom restlichen Netzwerk / Internet getrennt (z.B. Firewall zwischen Leittechniknetz und privatem Netzwerk)

- Firewall nach dem *Minimalprinzip** konfigurieren. Steuerungssysteme dürfen nur auf unbedingt notwendige Anlagenkomponenten zugreifen. Steuerungskomponenten dürfen keinen Internetzugang haben. Sollte ein Fernwartungszugriff vom Hersteller notwendig sein, ist dieser über einen speziell gesicherten Rechner (*Jumphost**) zu realisieren. Sämtliche Zugriffe müssen dokumentiert werden.

5. Fernzugänge / Fernwartung

Kategorie: 3 - 4

Mindestanforderung bei zwingend benötigten Fernzugängen für eigene Mitarbeiter oder Dienstleister: **Kein direkter Zugang** in das Leittechniknetz, sondern strikte mehrstufige Absicherung der Fernzugänge für Bediener, unter anderem durch:

- *VPN** über einen Zugangspunkt, idealerweise mit Multi-Faktor-Authentifizierung und personalisierten Zugangsdaten
- *Firewall-Regeln** für den Fernzugang nach dem Minimalprinzip
- Überwachung und Dokumentation des Fernzugriffs

Soweit betrieblich möglich, sollte für Fernzugänge geprüft werden, ob ein Lesezugriff ausreichend ist und damit auf aktive Steuerungsmöglichkeiten verzichtet werden kann. Falls die Möglichkeit der Fernsteuerung genutzt wird, soll ein ausschließlich für diese Tätigkeit bestimmtes, abgesichertes Endgerät genutzt werden.

- Multi-Faktor-Authentifizierung bei Fernzugängen inkl. VPN
- Fernwartung nur unter Aufsicht des Betreibers, IP-Freischaltungen an der Firewall nur für den IP-Netzbereich des Dienstleisters

6. Autorisierung / Manipulationsschutz

Kategorie: 3 - 4

Es muss sichergestellt sein, dass Zugriffe und Zugänge zu Prozessleittechnik-Systemen ausschließlich durch autorisierte Mitarbeiter möglich sind. Dadurch wird gewährleistet, dass nur für diese Aufgabe geschulte Mitarbeiter Änderungen an diesen Systemen vornehmen können und unerwünschte Änderungen (versehentlich oder vorsätzlich) ausgeschlossen sind. Es ist eine ausreichende PIN- bzw. Passwortkomplexität erforderlich, Standardkennwörter/-PINs sind zu ändern und ausschließlich sicher zu hinterlegen (z.B. mit Hilfe eines Passwortmanagers). Gebäude, Schaltschränke, Schnittstellen und Messsonden sind vor unbefugtem Zutritt / Zugriff zu schützen.

7. Updates

Kategorie: 3 - 4

Steuerungssysteme, welche nicht direkt mit dem Internet verbunden sind, sollten regelmäßig auf neue Updates geprüft und nach Möglichkeit sollten die Updates eingespielt werden. Die IT- und Steuerungskomponenten, welche direkt mit dem Internet verbunden sind, müssen auf aktuellem Stand gehalten werden. Auf einem Steuerungs-PC sollte ausschließlich die für den Betrieb benötigte Software installiert sein.

- Updates regelmäßig einspielen bei Betriebssystem, Software und insbesondere Fernwartungssoftware
- Bei Updates der Steuerungstechnik muss eine Funktionsprüfung des WKW stattfinden

8. Regelmäßige Systemprüfungen

Kategorie: 4

Betriebskritische Systeme sollten regelmäßig auf Ausfallsicherheit geprüft werden. Zudem sollten Logfiles der betriebskritischen Systeme sowie der zugehörigen Sicherheitssysteme sicher gespeichert werden. Die Logfiles sind für eventuell notwendige Analysen bei ungewöhnlichem Systemverhalten und IT-Sicherheitsvorfällen wichtig. Des Weiteren ist anzustreben, automatisierte Alarmierungen an die Administratoren / Zuständigen weiterzugeben.

- Regelmäßige Prüfung der Ausfallsicherheit (Funktionsprüfung von *USV/NEA** …)
- Logfiles regelmäßig sichern, Empfehlung hier diese mindestens 12 Monate vorzuhalten

Weiterführendes Thema für größere Organisationen: Informationssicherheitsmanagementsystem (ISMS)

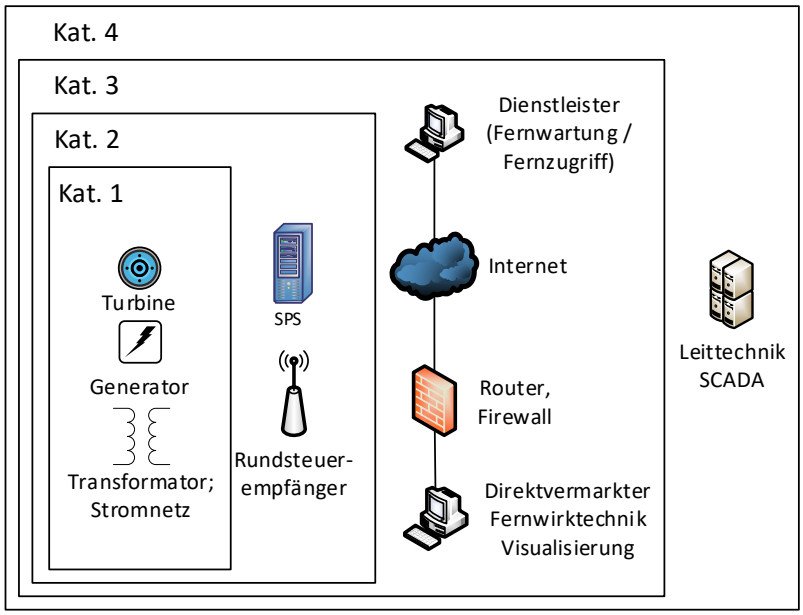
Kategorie: 4 (nur größere WKW)

Neben technischen Maßnahmen gibt es auch eine Reihe von betriebsinternen Prozessen, die sowohl zur Stärkung der IT-Sicherheit als auch zur Vorbereitung auf einen IT-Sicherheitsnotfall im Voraus abgeklärt werden sollten. Von großer Bedeutung ist die Festlegung von Verantwortlichkeiten.

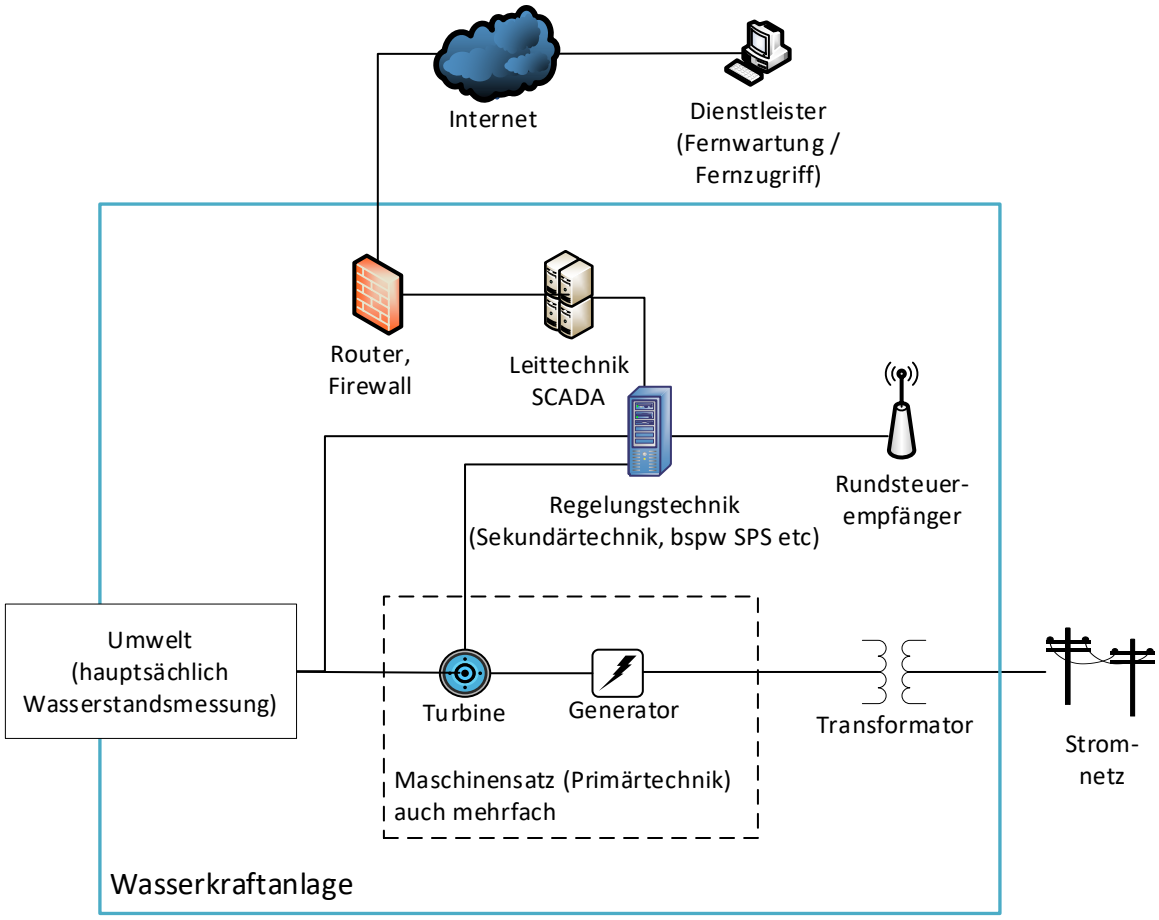
- Der Betreiber oder die Unternehmensleitung trägt die Gesamtverantwortung für die Anlage
- Sind wichtige IT-Sicherheitsaspekte (Leitlinien, Richtlinien, Alarmierungspläne, Notfallpläne, Wiederanlaufpläne etc.) den Mitarbeitern bekannt und zugänglich?
- Ist definiert, welche Personen und ggf. welche externen Stellen bei einem IT-Sicherheitsvorfall informiert werden (Alarmierungspläne)?

Es sollte festgelegt sein, wie bei einem Verdacht auf einen IT-Sicherheitsvorfall weiter vorgegangen wird, damit so schnell wie möglich reagiert werden kann und mögliche Folgen eingedämmt werden können. Dazu sollte ein Notfallmanagementkonzept für Ihre Anlage vorliegen. Dieses sollte Punkte wie Wiederherstellungsplan, Notfallhandbuch, Krisenkommunikation und Wiederanlaufplan enthalten.

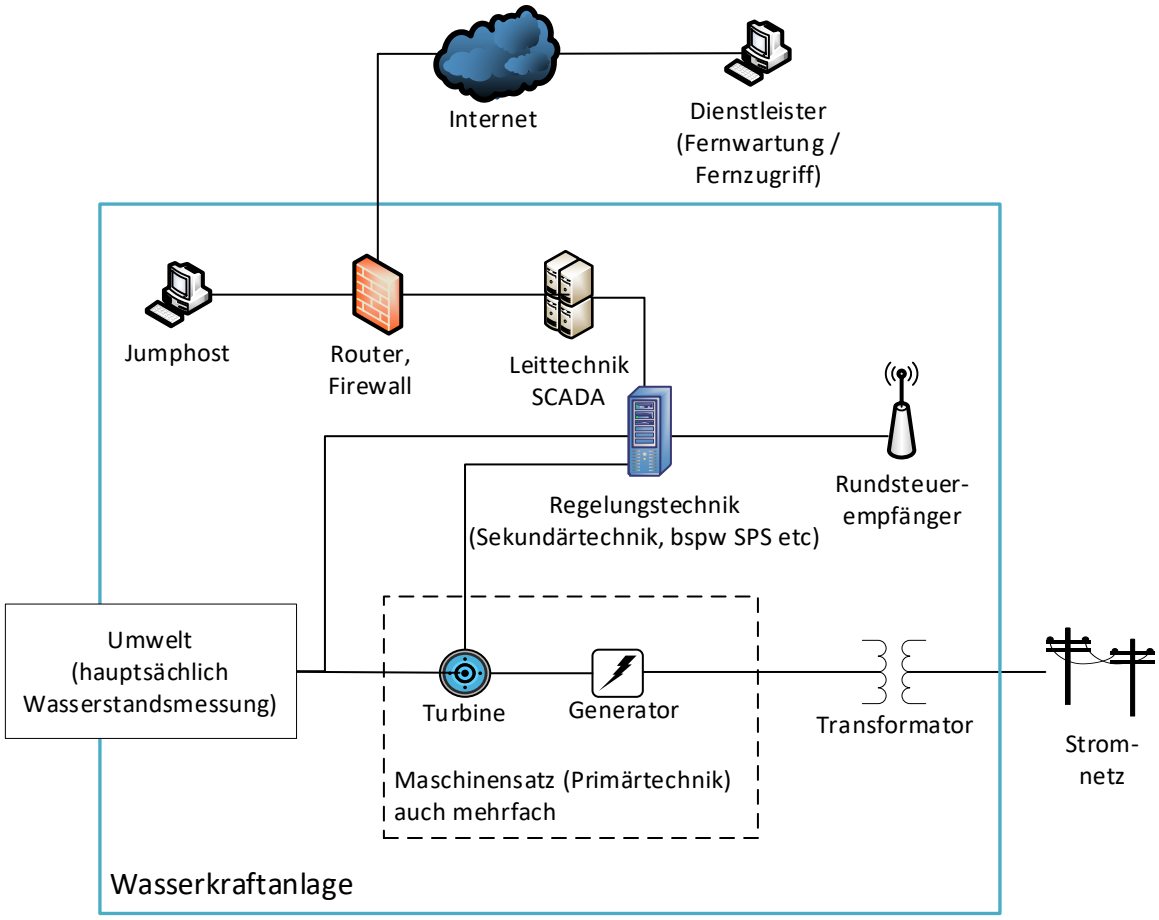
Grafische Darstellung der Kategorien (schematische Darstellung der Technikkomponenten)



Beispiel: Netzplan



Beispiel: Netzplan mit Sprung-PC (Jumphost)



Glossar

VPN	Virtuelles privates Netzwerk, eine gesicherte Verbindung von außen in ein Netzwerk
Firewall-Regeln	Konfigurationen auf der Firewall, die bestimmen, welche Komponenten unter welchen Bedingungen innerhalb eines Netzwerks miteinander kommunizieren dürfen.
Jumphost	Ein Jumphost (Sprung-Server) ermöglicht den Zugang zu einem Rechnernetzwerk, das durch eine Firewall getrennt und besonders geschützt ist (Netztrennung). Über diesen Zugang können z.B. Fernwartungszugriffe sicher realisiert werden.
Fernzugänge	Zugriffe von außen ins interne Netzwerk
Multi-Faktor-Authentifizierung (MFA)	mehrstufiges Verfahren zur Authentifizierung (besteht immer aus mehreren Faktoren, z.B. Passwort + Code per SMS aufs Mobiltelefon)
Minimalprinzip	Regeln und Berechtigungen so restriktiv wie möglich gestalten (z.B. für Firewall)
USV	unterbrechungsfreie Stromversorgung
NEA	Netzersatzanlage