Lastenheft und Pflichtenheft

Client-Server-Netzwerkinfrastruktur

Projekt: Planung und Implementierung einer zielgruppenorientierten Client-Server-Netzwerkinfrastruktur

Lernfeld 5: Rechnernetze nach Vorgaben einrichten

Projektdauer: 100 Stunden

Abgabeschluss: 15.12.2025

TEIL 1: LASTENHEFT

1. Einführung

Dieses Lastenheft beschreibt die Anforderungen und Ziele für die Planung und Implementierung einer Client-Server-Netzwerkinfrastruktur im Rahmen der ITA-Ausbildung. Das Projekt umfasst eine theoretische Gesamtplanung sowie eine praktische Umsetzung mit Hypervisor, NAS und Router.

2. Ausgangssituation

Ein mittelständisches Unternehmen benötigt eine moderne IT-Infrastruktur zur Unterstützung von circa 30-50 Mitarbeitern. Die bestehende IT-Infrastruktur ist veraltet oder nicht vorhanden und soll durch eine professionelle Client-Server-Architektur ersetzt werden.

Im Rahmen des Projekts wird die vollständige Infrastruktur theoretisch geplant. Für die praktische Demonstration werden mindestens ein Hypervisor, ein NAS-System und ein Router eingesetzt, um die Machbarkeit des Konzepts zu beweisen.

3. Zielsetzung

Das Projekt verfolgt folgende übergeordnete Ziele:

- Planung einer vollständigen IT-Netzwerkinfrastruktur mit Fokus auf Zuverlässigkeit und Skalierbarkeit
- Entwicklung eines durchdachten Sicherheitskonzepts
- Praktische Umsetzung einer funktionsfähigen Proof-of-Concept-Umgebung
- Dokumentation aller Planungs- und Implementierungsschritte
- Demonstration der erworbenen Kenntnisse im Bereich Netzwerktechnik

4. Funktionale Anforderungen

4.1 Netzwerkinfrastruktur

- Aufbau einer strukturierten Client-Server-Architektur
- Zentrale Datenspeicherung über NAS-System
- Virtualisierungsumgebung für flexible Server-Bereitstellung
- Netzwerksegmentierung für verschiedene Unternehmensbereiche

4.2 Serverdienste

- Cloud-Dienst für zentrale Dateiablage und Synchronisation
- Zentrale Benutzerverwaltung und Authentifizierung
- Backup- und Recovery-Lösungen
- Monitoring und Management-Tools

4.3 Client-Anbindung

- Unterstützung für Standard-Clients
- Netzwerkzugriff auf zentrale Ressourcen
- Zentrale Verwaltungsmöglichkeiten

5. Nicht-funktionale Anforderungen

5.1 Performance

- Gigabit-Ethernet als Standard für Client-Anbindung
- Schnelle Verbindungen zwischen Server-Komponenten
- Akzeptable Latenzzeiten im lokalen Netzwerk

5.2 Verfügbarkeit

- Ausfallsicherheit durch Virtualisierung
- Backup-Konzept mit definierten Recovery-Zeiten
- Stabile Netzwerkverbindungen

5.3 Sicherheit

- Firewall mit Zugriffskontrolle
- Netzwerksegmentierung durch VLANs
- Verschlüsselte Datenspeicherung für sensible Daten
- Regelmäßige Sicherheitsupdates

5.4 Skalierbarkeit

- Erweiterbarkeit für zusätzliche Arbeitsplätze
- Modularer Aufbau der Infrastruktur
- Flexible Storage-Erweiterung

6. Rahmenbedingungen

6.1 Technische Rahmenbedingungen

Theoretische Planung:

- Vollständige Enterprise-Infrastruktur ohne Budgetbeschränkung
- Berücksichtigung aktueller Standards und Best Practices
- Skalierbare Architektur für Wachstum

Praktische Umsetzung (Mindestausstattung):

- 1x Hypervisor-Server
- 1x NAS-System
- 1x Router mit Firewall-Funktionen
- Netzwerkkabel und Switches nach Verfügbarkeit
- Optional: Client-Systeme zur Demonstration

6.2 Organisatorische Rahmenbedingungen

- Projektdurchführung gemäß definierter Phasen
- Dokumentation aller Planungs- und Implementierungsschritte
- Abschlusspräsentation mit PowerPoint und Beamer
- Zeitbudget: 100 Stunden

7. Systemarchitektur (Überblick)

7.1 Netzwerktopologie

Die Netzwerktopologie umfasst verschiedene Segmente für unterschiedliche Zwecke:

- Management-Netz für Verwaltungsaufgaben
- Server-Netz für virtuelle Maschinen und Dienste
- Storage-Netz für Datenspeicherung
- Client-Netz für Endanwender

7.2 Server-Infrastruktur

- Virtualisierungs-Host für flexible Server-Bereitstellung
- Zentrales Storage-System für Datenablage
- Separate Netzsegmente für verschiedene Aufgaben

7.3 Sicherheitsarchitektur

- Firewall für Zugriffskontrolle
- Netzwerksegmentierung durch VLANs
- Verschlüsselung sensibler Verbindungen

8. Benutzergruppen und Anwendungsfälle

8.1 Benutzergruppen

- Administratoren mit Vollzugriff auf alle Systeme
- Fachabteilungen mit Zugriff auf spezifische Ressourcen
- Gäste mit eingeschränktem Internetzugang

8.2 Typische Anwendungsfälle

- Zugriff auf Cloud-Dienst für Dateiablage und -synchronisation
- Anmeldung über zentrale Benutzerverwaltung
- Zentrale Datensicherung und Wiederherstellung
- Bereitstellung neuer virtueller Server

9. Schnittstellen

9.1 Interne Schnittstellen

- Hypervisor-Management-Schnittstellen
- Storage-Protokolle (NFS, SMB)
- Authentifizierungssysteme

9.2 Externe Schnittstellen

- Internet-Anbindung über Provider-Router
- Optional: VPN-Verbindungen für Remote-Zugriff

10. Projektphasen

Phase	Beschreibung	Zeitaufwand
1	Planung und Recherche	ca. 20 Std.
2	Theoretische Durchführung	ca. 35 Std.
3	Praktische Durchführung	ca. 30 Std.
4	Auswertung und Ausblick	ca. 10 Std.
5	Präsentationserstellung	ca. 5 Std.

Table 1: Zeitplanung der Projektphasen

11. Abnahmekriterien

11.1 Theoretische Planung

- Vollständige Netzwerkdokumentation mit Topologie-Diagrammen
- Hardware- und Software-Spezifikationen
- Adressierungskonzept (IP-Plan)
- Sicherheitskonzept
- Kostenschätzung

11.2 Praktische Umsetzung

- Funktionierende Hypervisor-Umgebung mit mindestens zwei VMs
- NAS-System mit eingerichteten Dateifreigaben
- Konfigurierter Router mit Firewall
- Netzwerkverbindung zwischen allen Komponenten
- Dokumentation der Konfiguration

12. Lieferumfang

- Lastenheft (dieses Dokument)
- Pflichtenheft mit detaillierter technischer Spezifikation
- Netzwerkdiagramme und Topologie-Pläne
- Konfigurationsdokumentation
- Präsentationsunterlagen
- Optional: Funktionierende Test-Umgebung

TEIL 2: PFLICHTENHEFT

1. Einleitung

Dieses Pflichtenheft beschreibt die technische Umsetzung der im Lastenheft definierten Anforderungen. Es dient als Grundlage für die Implementierung der Netzwerkinfrastruktur und definiert konkrete technische Lösungen für die praktische Umsetzung.

2. Soll-Kriterien (Zwingende Anforderungen)

Die folgenden Anforderungen müssen zwingend umgesetzt werden, um das Projektziel zu erreichen:

2.1 Theoretische Planung (Soll)

- Vollständige Dokumentation der Netzwerkarchitektur
- VLAN-Design mit mindestens 3 Segmenten
- IP-Adressplan für alle Netzwerkbereiche
- Sicherheitskonzept mit Firewall-Regeln
- Backup-Strategie

2.2 Praktische Umsetzung (Soll)

- Installation und Konfiguration eines Hypervisors
- Betrieb von mindestens 2 virtuellen Maschinen
- Integration eines NAS-Systems mit Dateifreigaben
- Konfiguration eines Routers mit Firewall-Funktionen
- Netzwerkverbindung zwischen allen Komponenten
- Cloud-Dienst für zentrale Dateiablage funktionsfähig
- Zentrale Benutzerverwaltung implementiert

2.3 Serverdienste (Soll)

- Cloud-Lösung für Dateisynchronisation und -ablage
- Zentrales Authentifizierungssystem für Benutzerverwaltung
- Basis-Monitoring der Infrastruktur

2.4 Sicherheit (Soll)

- Firewall-Konfiguration mit Zugriffskontrolle
- Netzwerksegmentierung durch VLANs
- Sichere Administrationszugänge (SSH, HTTPS)

3. Kann-Kriterien (Optional)

Die folgenden Anforderungen können bei ausreichender Zeit und Ressourcen zusätzlich umgesetzt werden:

3.1 Erweiterte Funktionen (Kann)

- VPN-Lösung für Remote-Zugriff
- Erweiterte Monitoring-Lösung mit Grafana-Dashboards
- Automatisierte Backup-Jobs mit Benachrichtigungen
- Container-Plattform (Docker/Kubernetes)
- WLAN-Integration mit Access Points
- Hochverfügbarkeits-Features (HA)

3.2 Zusätzliche Serverdienste (Kann)

- Webserver für interne Dienste
- Mail-Server für interne Kommunikation
- Git-Server für Versionsverwaltung
- Wiki oder Dokumentations-Plattform
- Ticketsystem für IT-Support

3.3 Sicherheitserweiterungen (Kann)

- Intrusion Detection System (IDS)
- Verschlüsselung der Datenspeicherung
- Zwei-Faktor-Authentifizierung
- Zentrale Log-Aggregation mit SIEM
- Regelmäßige Vulnerability-Scans

3.4 Performance-Optimierungen (Kann)

- SSD-Cache für Storage
- Load-Balancing zwischen VMs
- QoS-Konfiguration für Netzwerkpriorisierung
- Dedizierte 10-Gigabit-Verbindungen

4. Abgrenzungskriterien (Nicht im Scope)

Die folgenden Aspekte sind explizit **nicht** Teil dieses Projekts:

4.1 Hardware

- Beschaffung und Kauf von Hardware (wird gestellt)
- Rechenzentrumsinfrastruktur (Klimatisierung, USV-Systeme)
- Client-Hardware oder End-User-Geräte
- Physische Sicherheitsmaßnahmen (Zutrittskontrolle, Videoüberwachung)

4.2 Software und Lizenzierung

- Beschaffung kommerzieller Software-Lizenzen
- Enterprise-Support-Verträge
- kostenpflichtige Cloud-Dienste oder SaaS-Lösungen

4.3 Betrieb und Support

- Langfristiger Produktivbetrieb nach Projektende
- 24/7-Support oder On-Call-Dienste
- Schulungen für Endanwender
- Service-Level-Agreements (SLAs)

4.4 Anwendungen und Systeme

- Desktop-Anwendungen oder Client-Software
- ERP-, CRM- oder andere Business-Systeme
- Telefonie-Infrastruktur (VoIP)
- Druckerinfrastruktur und Print-Server
- Mobile Device Management (MDM)

4.5 Externe Anbindungen

- Internet-Provider-Verträge
- Cloud-Provider-Integration (AWS, Azure, etc.)
- Externe Rechenzentrumsanbindungen
- B2B-Netzwerkverbindungen zu Partnern

4.6 Compliance und Zertifizierung

- DSGVO-Compliance-Audit

- ISO-27001-Zertifizierung
- Penetrationstests durch externe Dienstleister
- Rechtsberatung zu IT-Sicherheit

5. Systemarchitektur - Detailplanung

2.1 Netzwerk-Topologie

Logische Struktur (VLAN-Design):

VLAN	Verwendung
VLAN 1	Management (192.168.1.0/24)
VLAN 10	Server-Infrastruktur (192.168.10.0/24)
VLAN 20	Storage-Netzwerk (192.168.20.0/24)
VLAN 100	Client-Netzwerk (10.0.100.0/24)

Table 2: VLAN-Zuordnung und IP-Bereiche

2.2 Hardware-Spezifikation (Praktische Mindest-Implementierung)

Router:

- Router mit Firewall-Funktionen oder dedizierte Firewall-VM
- Gigabit-Ethernet-Ports
- VLAN-Unterstützung
- NAT und Portweiterleitung

Hypervisor-Server:

- Server-Hardware nach Verfügbarkeit
- Virtualisierungsplattform (z.B. Proxmox VE, VMware ESXi oder vergleichbar)

NAS-System:

- NAS-Hardware nach Verfügbarkeit
- NAS-Betriebssystem (z.B. TrueNAS, OpenMediaVault oder vergleichbar)
- RAID-Konfiguration für Datensicherheit

Netzwerk-Komponenten:

- Router mit Firewall-Funktionen
- Netzwerkverkabelung nach Bedarf

- Optional: Managed Switch für VLAN-Unterstützung

3. Software-Komponenten

3.1 Hypervisor und Virtualisierung

Primäre Lösung: Proxmox VE

- Typ: Type-1-Hypervisor (Bare-Metal)
- Features: KVM-Virtualisierung, LXC-Container
- Management: Web-GUI und CLI
- Lizenz: Open Source

3.2 NAS-Betriebssystem

Primäre Lösung: TrueNAS Core

- ZFS-Dateisystem für Datenintegrität
- Snapshots und Replikation
- Protokolle: NFS, SMB
- Web-basierte Verwaltung

3.3 Virtuelle Maschinen (Beispiele)

VM 1: Cloud-Dienst

- Bereitstellung einer Cloud-Lösung für zentrale Dateiablage
- Beispiele: Nextcloud, ownCloud oder vergleichbare Lösungen
- Web-basierter Zugriff und Synchronisation

VM 2: Zentrale Benutzerverwaltung

- Authentifizierungs- und Autorisierungssystem
- Beispiele: Active Directory, LDAP, FreeIPA oder vergleichbar
- Zentrale Verwaltung von Benutzerkonten und Berechtigungen

VM 3: Monitoring-Server

- Überwachung der Infrastruktur
- Beispiele: Zabbix, Prometheus/Grafana oder vergleichbar

3.4 Firewall und Routing

- pfSense oder OPNsense als Firewall-VM
- Inter-VLAN-Routing
- NAT für Internet-Zugang

- Firewall-Regeln für Zugriffskontrolle

4. Netzwerk-Konfiguration

4.1 IP-Adressplan (Beispiel)

Management-Netz (VLAN 1):

- 192.168.1.1 - Router/Gateway
- 192.168.1.20 - Hypervisor Management-Interface
- 192.168.1.30 - NAS Management-Interface

Server-Netz (VLAN 10):

- 192.168.10.1 - Virtual Router (pfSense VM)
- 192.168.10.20 - Dateiserver VM
- 192.168.10.30 - Monitoring Server VM

Storage-Netz (VLAN 20):

- 192.168.20.10 - Hypervisor Storage-Interface
- 192.168.20.20 - NAS Storage-Interface

Client-Netz (VLAN 100):

- 10.0.100.1 - Gateway
- 10.0.100.50-250 - DHCP-Bereich

4.2 Routing und Firewall

Inter-VLAN-Routing:

- Virtual Firewall (pfSense/OPNsense VM) als Router zwischen VLANs
- Firewall-Regeln für kontrollierten Zugriff
- Management-VLAN nur von Admin-PCs erreichbar
- Storage-VLAN isoliert

Firewall-Regeln (Beispiele):

- Clients → Server: HTTP/HTTPS, SMB erlaubt
- Clients → Internet: Erlaubt via NAT
- Server → Storage: NFS erlaubt
- Management → Alle: Erlaubt für Administration
- Default: Deny All
-

5. Storage-Konzept

5.1 NAS-Konfiguration

RAID-Setup:

- RAID 5 für Datenintegrität
- Beispiel: 4x 4 TB in RAID 5 = ca. 12 TB nutzbar

Storage-Pools und Shares:

- Pool 1: Produktivdaten (NFS/SMB)
- Pool 2: Backups (NFS für Proxmox Backup)
- Pool 3: ISO-Images und Templates

Protokolle:

- NFS v4: Für Linux-VMs und Hypervisor-Datastores
- SMB/CIFS: Für Windows-Clients und VMs

5.2 Hypervisor-Storage

Lokaler Storage:

- System-Disk: Proxmox VE Installation
- VM-Disk-Pool: Schnelle VMs auf lokalem SSD

Network-Storage:

- NFS-Mount vom NAS für VM-Storage
- Shared Storage für flexible VM-Verwaltung

5.3 Backup-Strategie

Proxmox Backup:

- Automatische VM-Backups auf NAS
- Retention: 7 Tage täglich, 4 Wochen wöchentlich
- Backup-Window: 02:00-06:00 Uhr

NAS-Backup:

- Snapshots: Stündlich (24h), täglich (7d), wöchentlich (4w)
- Optional: Externe Replikation auf zweites NAS

6. Sicherheitskonzept

6.1 Netzwerksicherheit

Segmentierung:

- Strikte VLAN-Trennung
- Firewall zwischen allen Segmenten
- Storage-VLAN komplett isoliert

Access Control:

- Port-basierte Zugriffskontrolle
- Firewall-Regeln nach Least-Privilege-Prinzip

6.2 System-Härtung

Hypervisor:

- Minimale Installation ohne unnötige Services
- Regelmäßige Updates über Update-Repositories
- Firewall auf Host-Ebene

VMs:

- Template-basierte VM-Erstellung mit gehärtetem Base-Image
- Automatische Sicherheitsupdates
- Minimale Software-Installation
- Host-basierte Firewall (ufw/firewalld)

NAS:

- Deaktivierung ungenutzter Dienste
- Verschlüsselte Admin-Zugriffe (HTTPS, SSH)
- Regelmäßige Firmware-Updates
- Audit-Logging aktiviert

6.3 Zugriffsschutz

Authentifizierung:

- Starke Passwort-Richtlinien
- SSH-Key-basierte Authentifizierung für Server

Verschlüsselung:

- TLS für alle Web-Services
- SSH für Remote-Administration
- Optional: Daten-at-Rest-Verschlüsselung auf NAS

7. Monitoring und Management

7.1 Monitoring-Lösung

Zabbix / Prometheus + Grafana:

- Monitoring aller Server, VMs, NAS
- Metriken: CPU, RAM, Disk, Network, Services
- Alerting via E-Mail
- Performance-Dashboards

Überwachte Komponenten:

- Hypervisor: Ressourcen-Auslastung, VM-Status
- NAS: Disk-Health (SMART), Pool-Status, Temperature
- VMs: Service-Verfügbarkeit, Logs

7.2 Zentrales Logging

- Zentrale Log-Sammlung von allen Systemen
- Retention: 90 Tage
- Log-Analyse mit Syslog-Server

8. Dokumentation

8.1 Technische Dokumentation

Zu erstellende Dokumente:

- Netzwerk-Topologie-Diagramm (physisch und logisch)
- IP-Adressplan
- VLAN-Konfiguration
- Hypervisor-Konfiguration
- NAS-Konfiguration und Share-Berechtigungen
- VM-Inventar mit Ressourcen und Zweck
- Firewall-Regelwerk
- Backup- und Recovery-Verfahren

Dokumentationsformat:

- Markdown oder PDF
- Netzwerkdiagramme mit draw.io oder Visio

8.2 Benutzer-Dokumentation

Administrator-Handbuch:

- Erste Schritte und Zugriff
- Routine-Wartungsaufgaben
- Backup und Recovery
- Troubleshooting-Leitfaden

9. Testing und Validierung

9.1 Funktionstests

Netzwerk-Tests:

- VLAN-Isolation testen (Ping zwischen VLANs)
- Bandbreiten-Tests (iperf3)
- Latenz-Messungen

Hypervisor-Tests:

- VM-Erstellung und Start
- Snapshot-Erstellung und Wiederherstellung
- Ressourcen-Limits testen

Storage-Tests:

- Lese-/Schreibgeschwindigkeit (dd, fio)
- NFS/SMB-Mount von Client
- Backup und Recovery

9.2 Performance-Tests

Benchmark-Tools:

- iperf3: Netzwerk-Durchsatz
- fio: Storage-Performance
- sysbench: CPU/RAM-Performance

Acceptance Criteria:

- Gigabit-Links: min. 900 Mbps Durchsatz
- VM-Boot-Zeit: max. 60 Sekunden
- Storage-Latenz: max. 10ms für Clients

9.3 Sicherheits-Tests

Vulnerability Scanning:

- Nmap für Port-Scans
- Testen der Firewall-Regeln
- Überprüfung der VLAN-Isolation

10. Implementierungs-Roadmap

Phase 1: Vorbereitung (5 Std.)

- Hardware bereitstellen
- Software herunterladen (ISOs, Images)
- Workspace einrichten

Phase 2: Basis-Installation (8 Std.)

- Hypervisor-Server aufbauen und Proxmox installieren
- NAS aufbauen und TrueNAS installieren
- Router konfigurieren
- Verkabelung herstellen

Phase 3: Netzwerk-Konfiguration (6 Std.)

- VLANs konfigurieren
- IP-Adressen vergeben
- Netzwerk-Tests durchführen

Phase 4: Storage-Setup (4 Std.)

- RAID auf NAS konfigurieren
- Storage-Pools und Shares erstellen
- NFS/SMB aktivieren und testen
- NFS-Datastore in Proxmox einbinden

Phase 5: VM-Deployment (6 Std.)

- VM-Templates erstellen
- VMs erstellen und OS installieren
- Basis-Konfiguration der VMs
- Netzwerk-Anbindung testen

Phase 6: Service-Konfiguration (8 Std.)

- Dateiserver konfigurieren
- Monitoring-System aufsetzen
- Firewall-VM konfigurieren

Phase 7: Testing und Dokumentation (8 Std.)

- Alle Funktionstests durchführen
- Performance-Messungen
- Sicherheits-Checks
- Dokumentation vervollständigen

Phase 8: Optimierung (5 Std.)

- Performance-Tuning
- Backup-Jobs einrichten
- Monitoring-Alerts konfigurieren
- Cleanup und Abnahme

Gesamtzeit praktische Umsetzung: ca. 50 Std.

11. Risiken und Gegenmaßnahmen

11.1 Technische Risiken

Risiko	Gegenmaßnahme
Hardware-Ausfall	USV für kritische Komponenten, Backup-Konzept
Performance-Engpässe	Performance-Tests, Skalierungsreserven
Kompatibilitätsprobleme	Hardware Compatibility Lists prüfen, Vorab-Tests

Table 3: Technische Risiken und Gegenmaßnahmen

11.2 Zeitliche Risiken

- Verzögerungen bei Hardware-Beschaffung: Frühzeitige Bestellung, Alternativen definieren
- Komplexitäts-Unterschätzung: Pufferzeiten einplanen, Scope auf Minimum reduzierbar

11.3 Projektrisiken

- Fehlende Kenntnisse: Vorab-Recherche, Online-Tutorials, Dokumentation
- Scope Creep: Klare Abgrenzung Must-Have vs. Nice-to-Have

12. Erweiterungsmöglichkeiten

12.1 Kurzfristig

- WLAN-Integration mit Access Points
- VPN-Lösung für Remote-Zugriff
- Erweiterte Backup-Strategie

12.2 Mittelfristig

- High-Availability-Cluster für Hypervisor
- Redundantes Storage-System
- Container-Orchestrierung

13. Abnahme und Übergabe

13.1 Abnahmekriterien

Theoretische Planung:

- Vollständiges Lastenheft
- Vollständiges Pflichtenheft
- Netzwerk-Topologie-Diagramme
- IP-Adressplan und VLAN-Design
- Sicherheitskonzept dokumentiert

Praktische Implementierung:

- Hypervisor installiert und konfiguriert
- NAS mit RAID und Shares eingerichtet
- Router mit Firewall konfiguriert
- Mindestens 2 VMs laufen stabil
- Netzwerkverbindung zwischen allen Komponenten
- Monitoring funktionsfähig
- Dokumentation der Konfiguration
- Funktionstests erfolgreich

13.2 Übergabedokumente

- Lastenheft und Pflichtenheft
- Technische Dokumentation
- Konfigurationsdateien-Backup
- Zugangsdaten-Dokumentation
- Präsentationsunterlagen
- Test-Protokolle

13.3 Präsentation (15-20 Minuten)

Agenda:

1. Projektvorstellung und Zielsetzung (3 Min.)
2. Theoretische Netzwerkplanung (5 Min.)
3. Praktische Implementierung - Demo (7 Min.)
4. Herausforderungen und Lessons Learned (3 Min.)
5. Ausblick und Erweiterungen (2 Min.)

Demo-Inhalte:

- Proxmox Web-GUI zeigen
- VM starten und stoppen
- NAS-Shares zeigen
- Firewall-Konfiguration
- Monitoring-Dashboard

Erstellt am: 18.11.2025

Version: 1.0

Status: Entwurf