

# MiMed Echtzeitmaster

## Bedienkonzept und Sicherheitsaspekte

**Christian Dietz**

GEFÖRDERT VOM

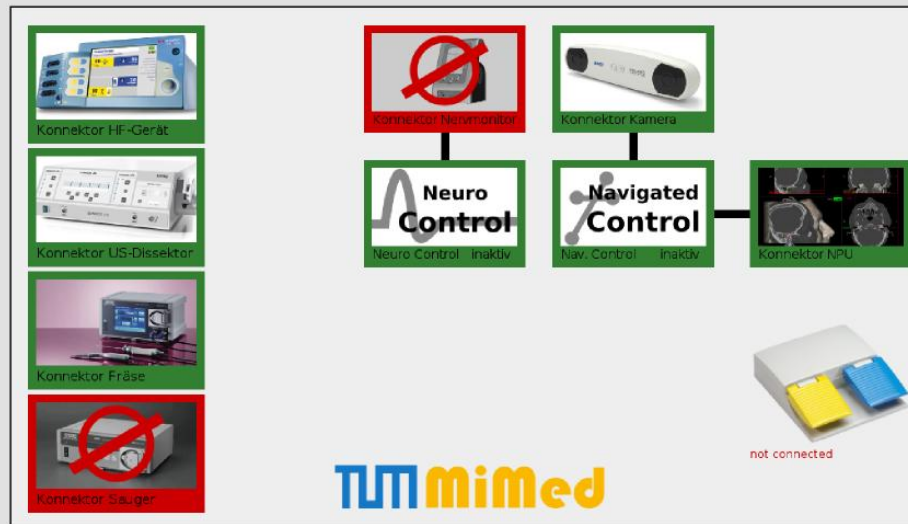


Bundesministerium  
für Bildung  
und Forschung

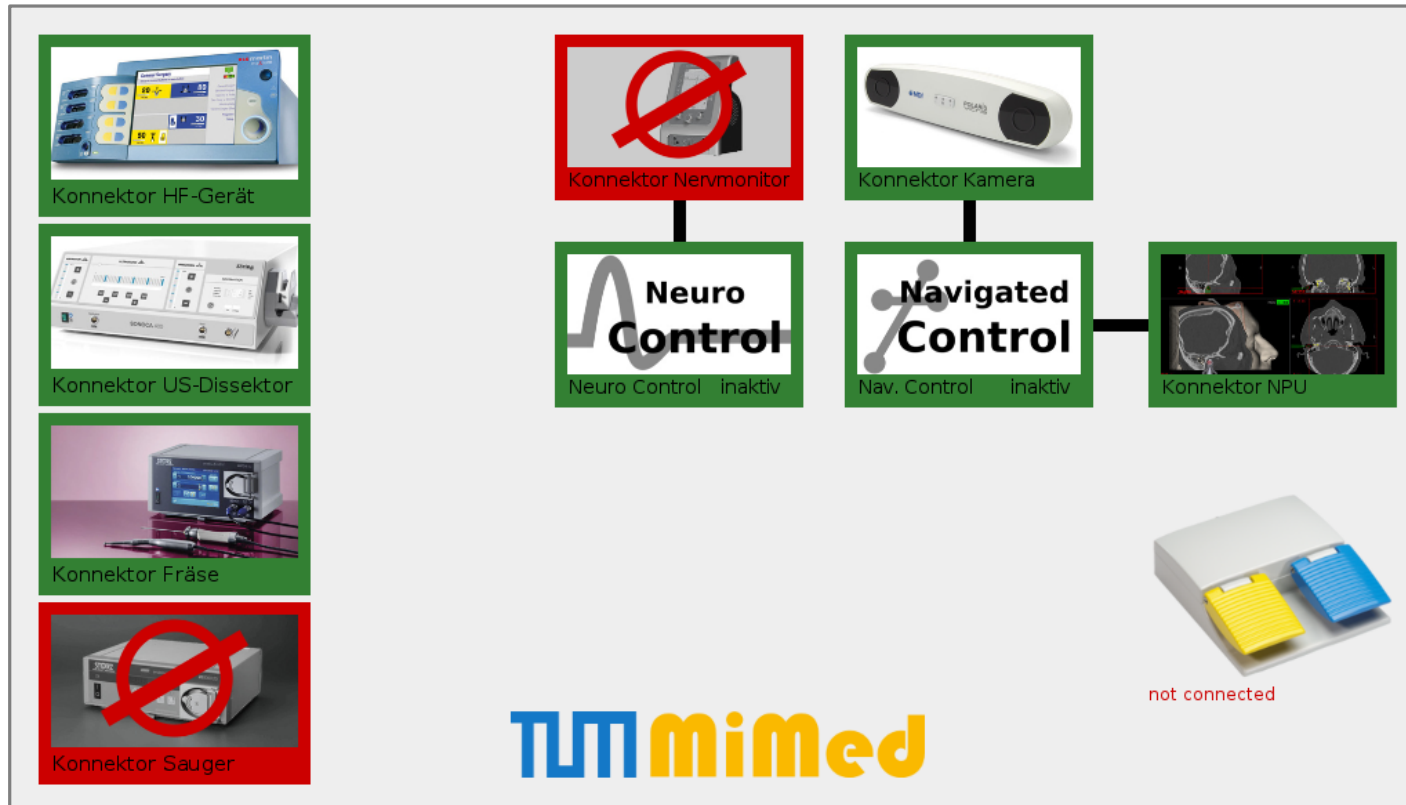
# MiMed Echtzeitmaster

## Bedienkonzept

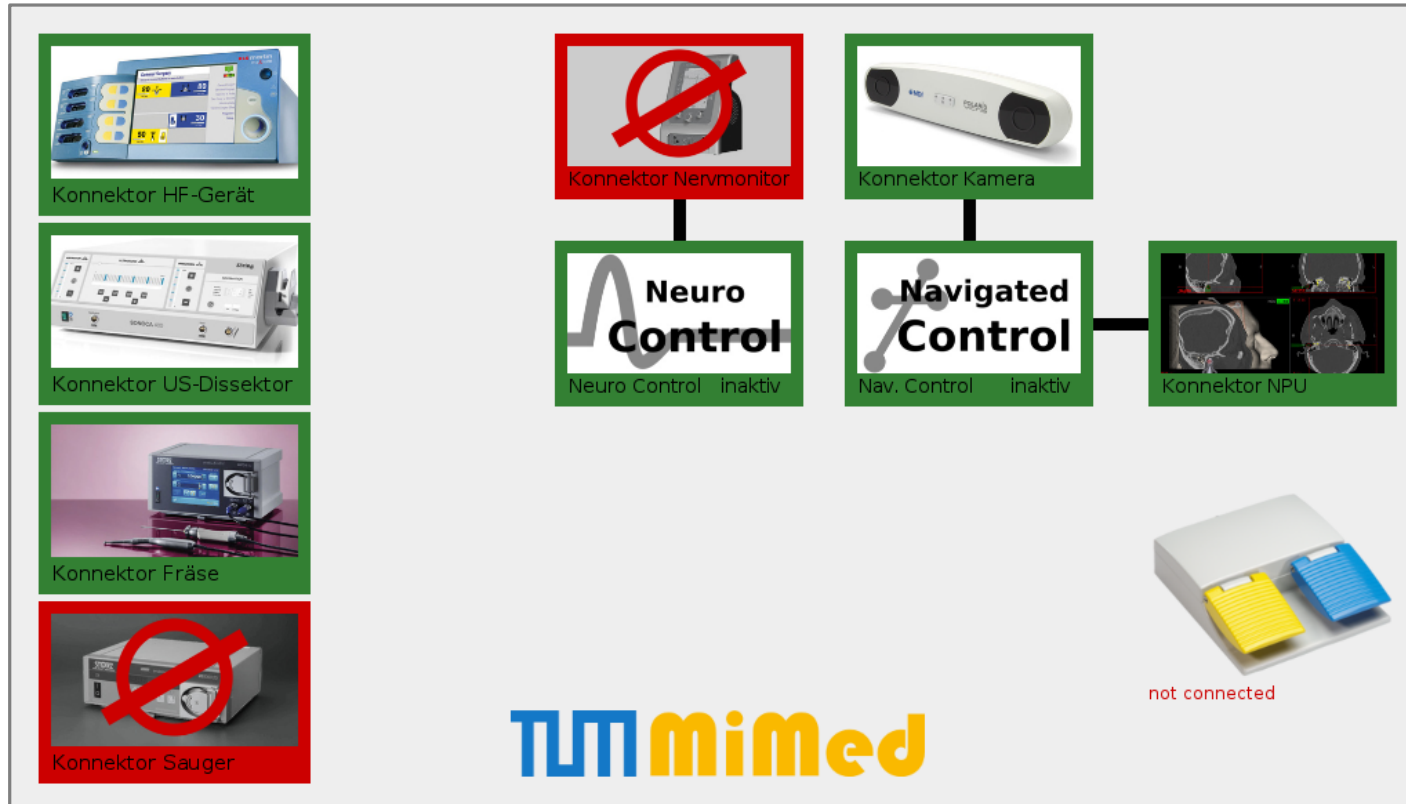
# Bedienkonzept Master



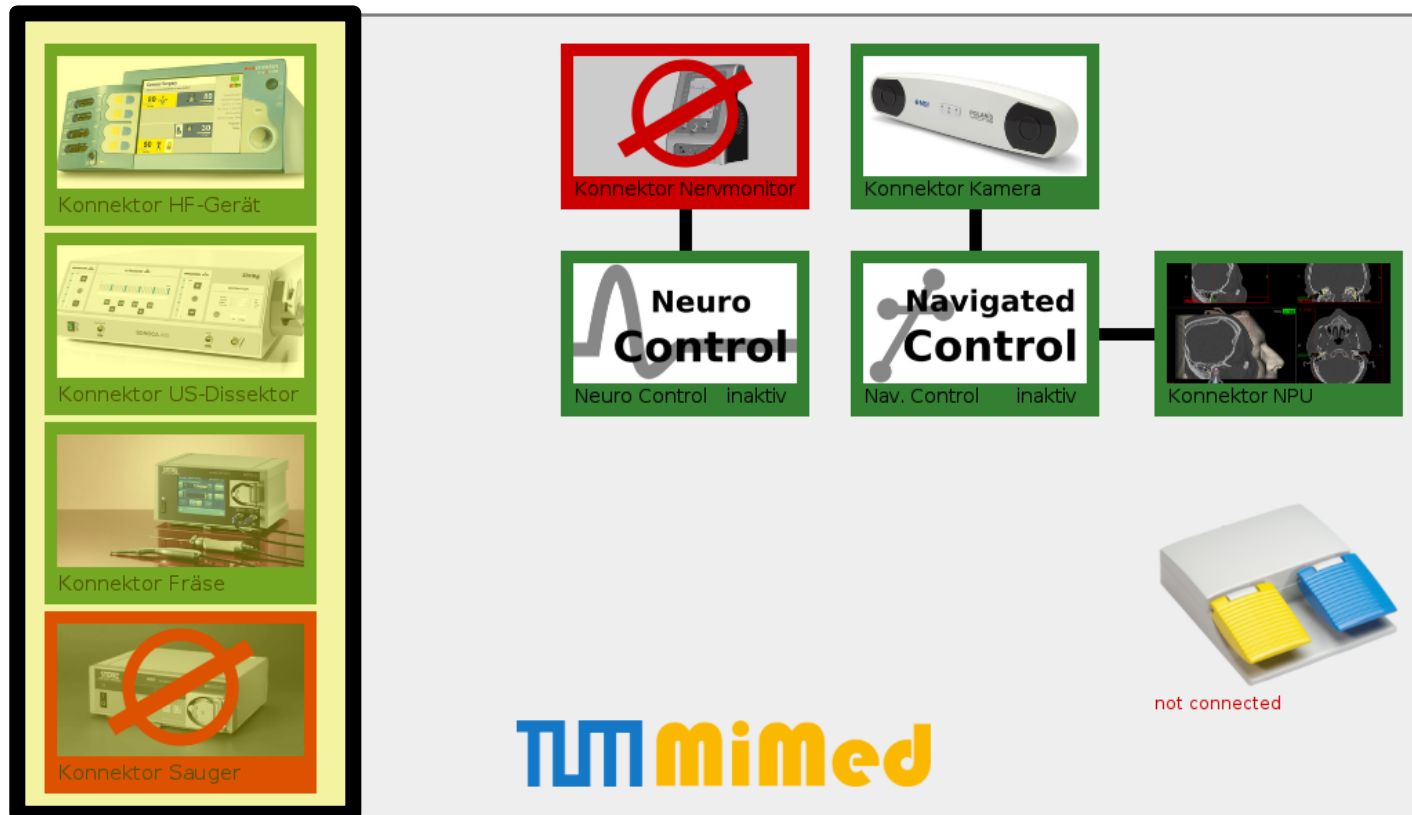
# Bedienkonzept Master



# Bedienkonzept Master

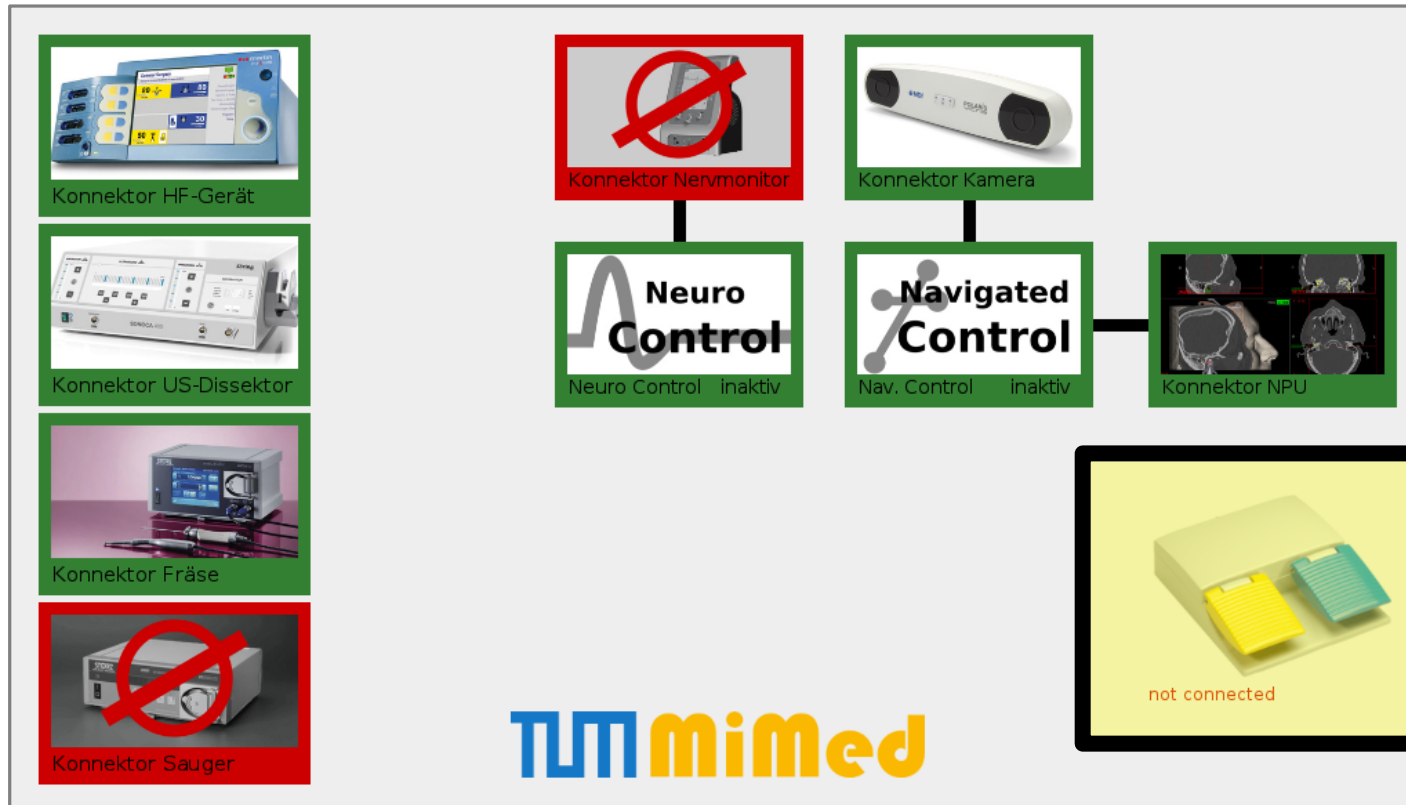


# Bedienkonzept Master



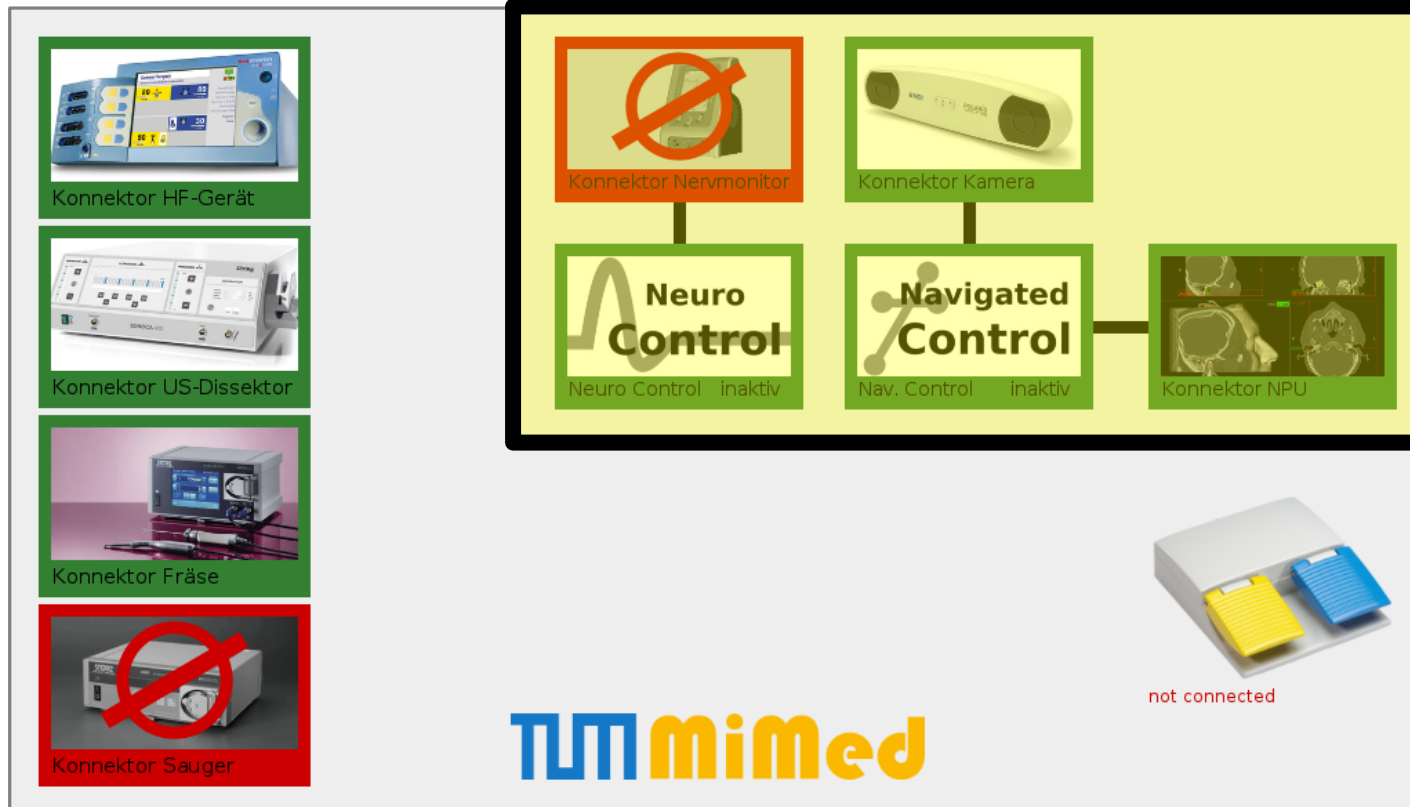
Steuerbare Geräte

# Bedienkonzept Master



Fußpedal

# Bedienkonzept Master



Assistenz-  
Systeme

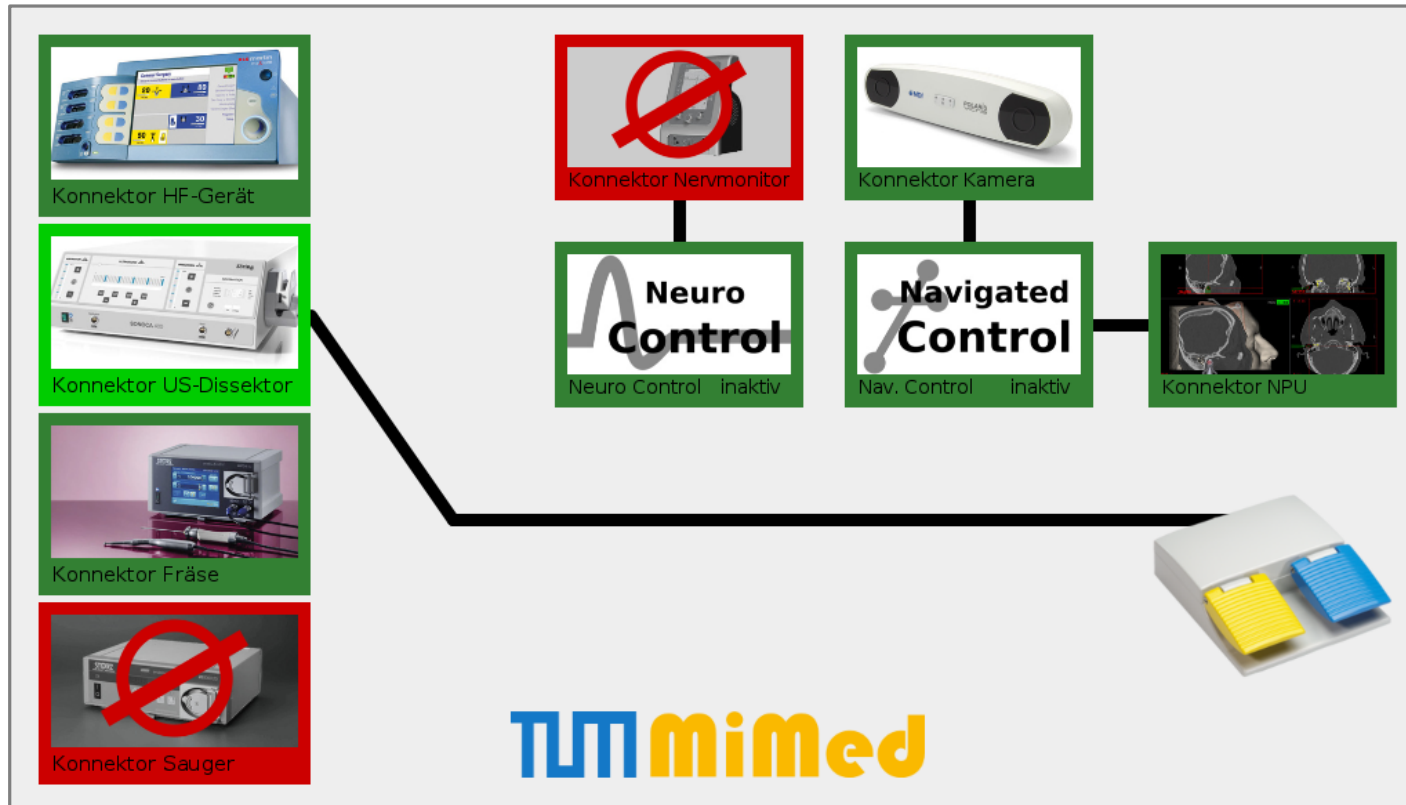


# Bedienkonzept Master



Auswahl des zu steuernden Gerätes mit „Touch“ auf das Gerät

# Bedienkonzept Master



Der aktuelle Verschaltungszustand wird angezeigt

# Bedienkonzept Master

Konnektor HF-Gerät

Konnektor Nervmonitor

Konnektor Kamera

**Umschalten nicht möglich**

**Gerät nicht verfügbar**

Ko

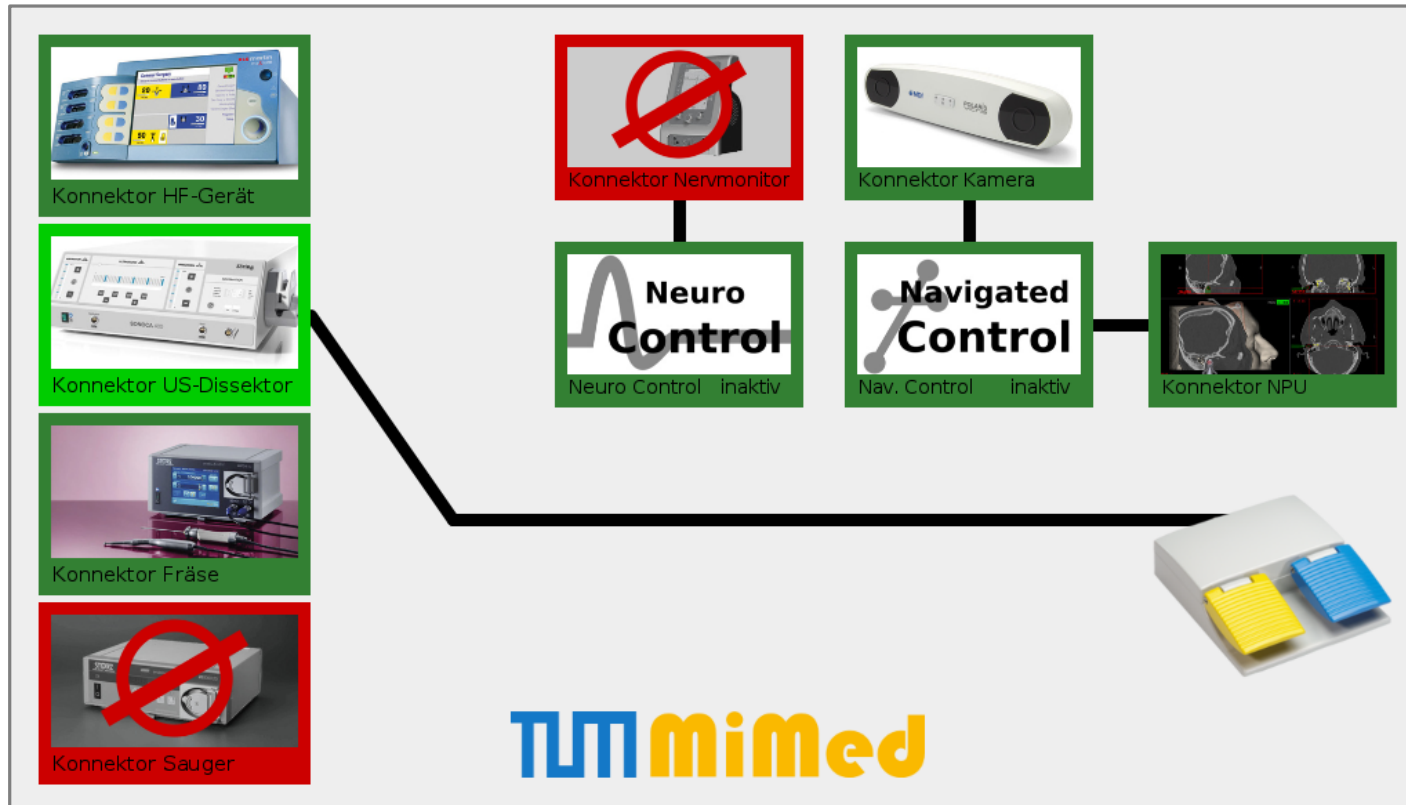
Ko

Konnektor Sauger

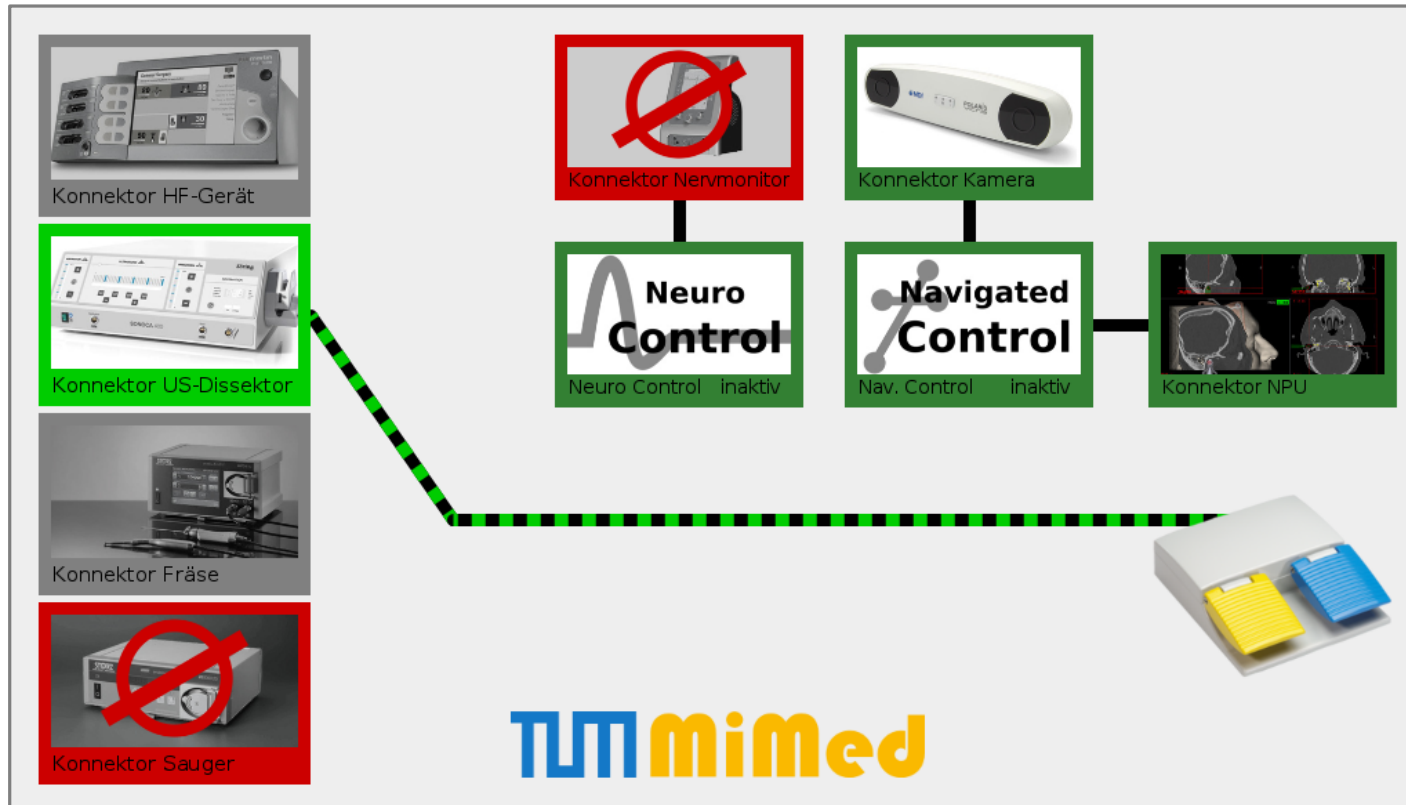
TUM mimed

Nur verfügbare Geräte können ausgewählt werden

# Bedienkonzept Master



# Bedienkonzept Master



Während Aktuierung ist kein Umschalten möglich

# Bedienkonzept Master



**Umschalten nicht möglich**  
**Pedal in Verwendung**

Konnektor HF-Gerät

Konnektor Nervmonitor

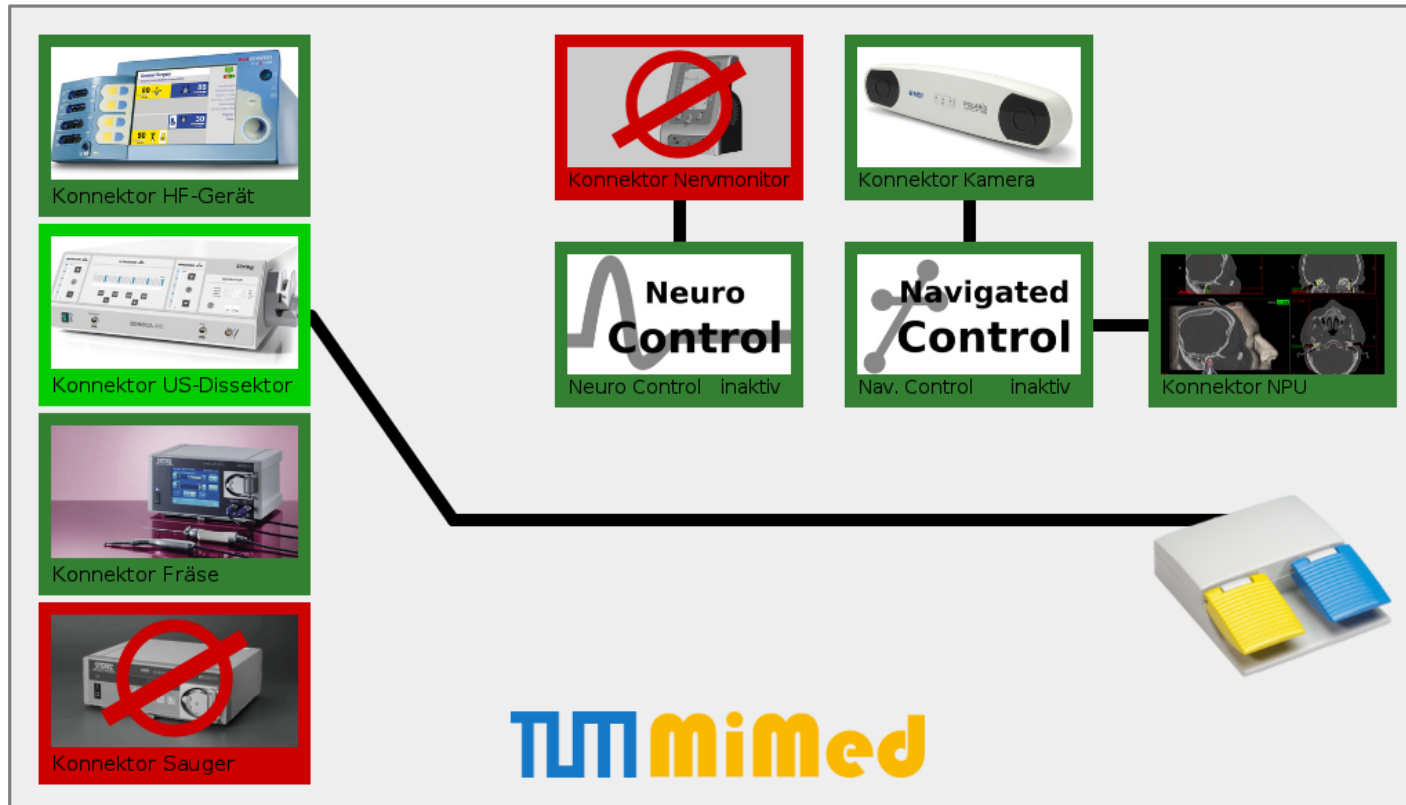
Konnektor Kamera

Konnektor Sauger

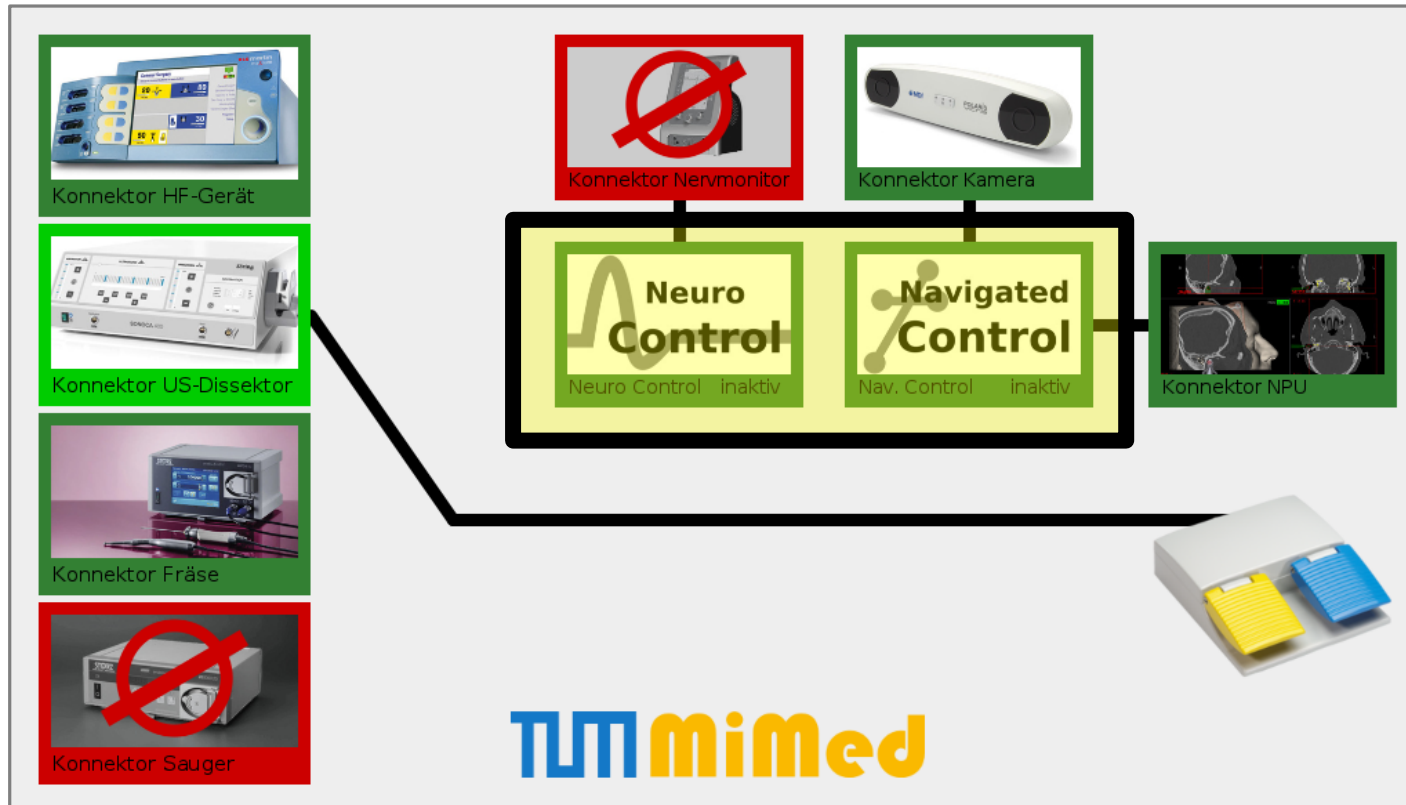
**TUM mimed**

Während Aktuierung ist kein Umschalten möglich

# Bedienkonzept Master



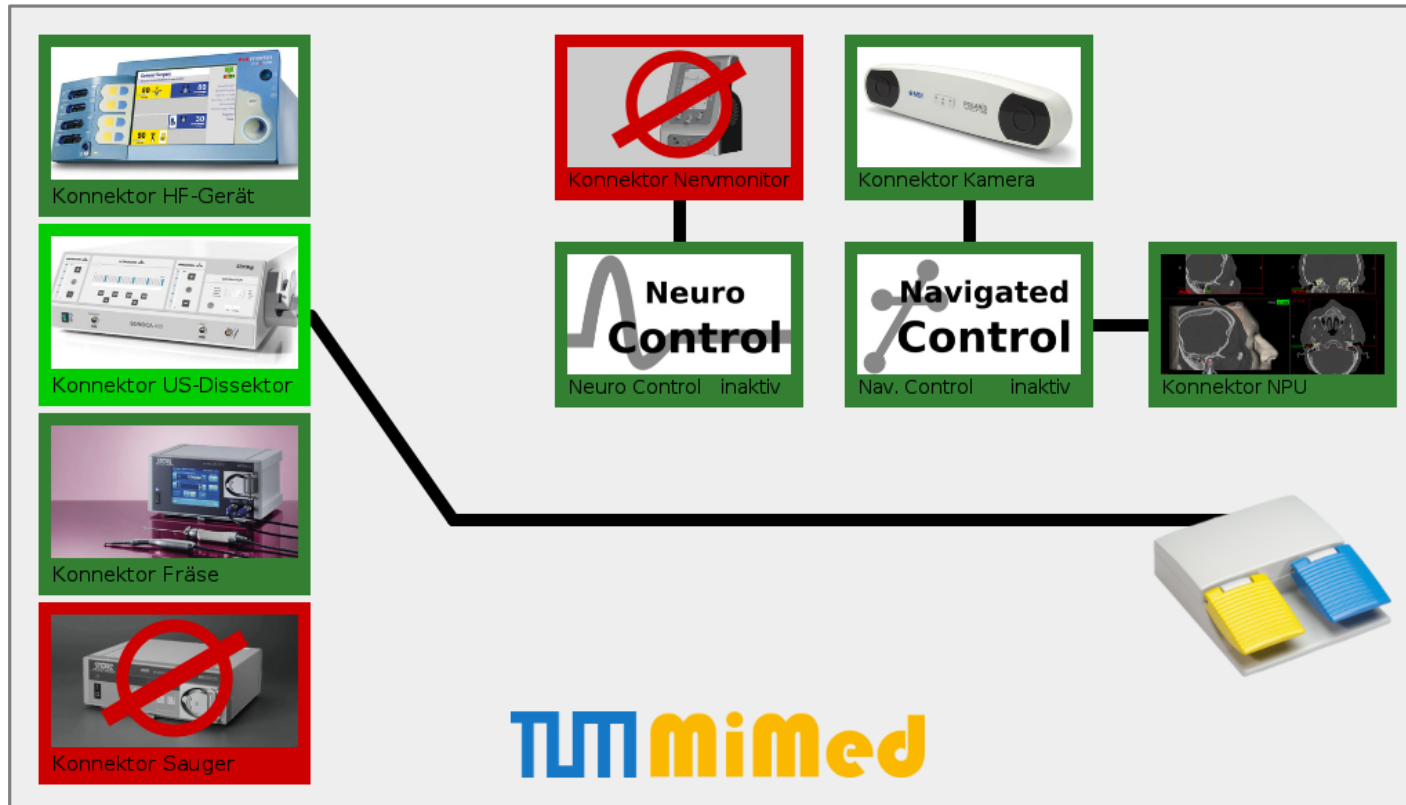
# Bedienkonzept Master



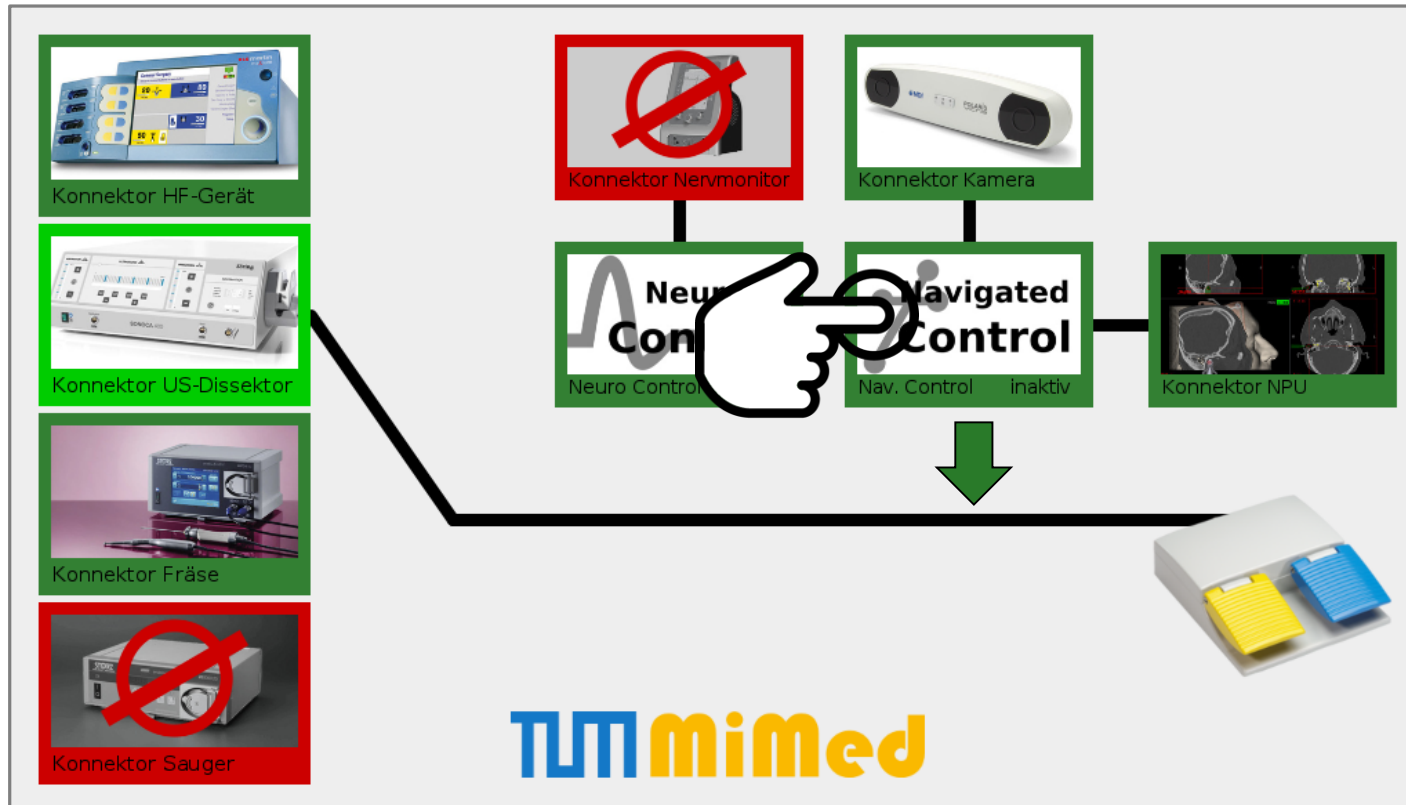
Funktionsmodule



# Bedienkonzept Master

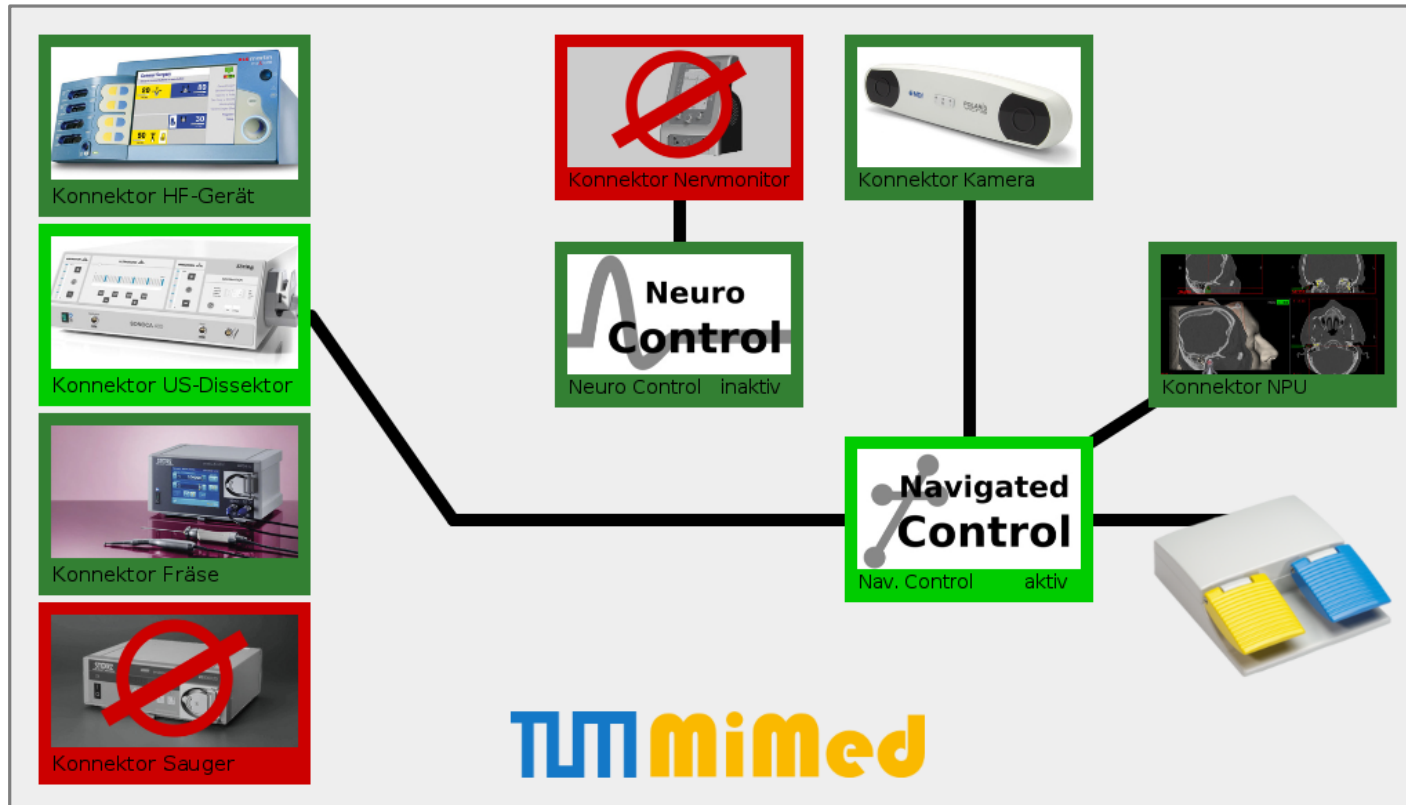


# Bedienkonzept Master



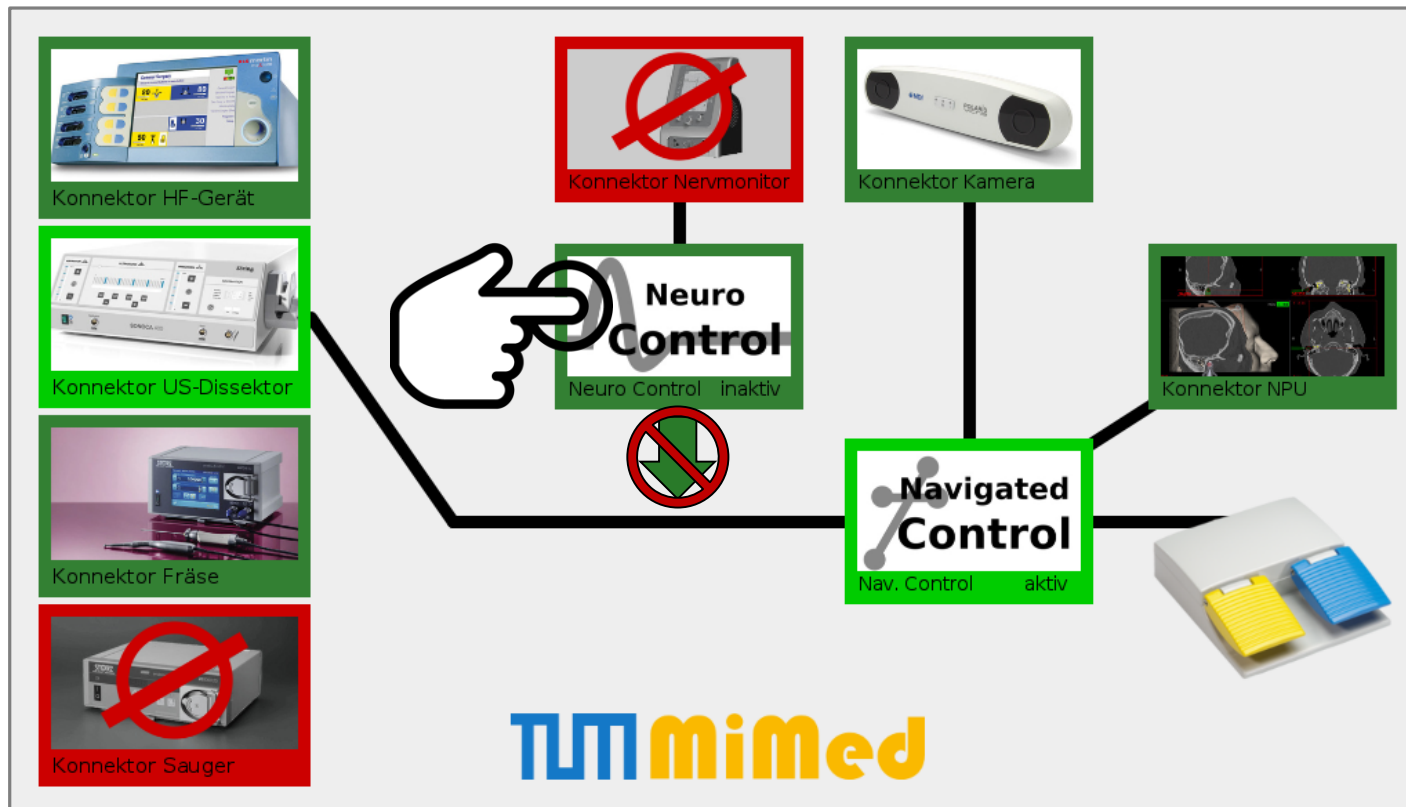
Aktivieren von Funktionsmodulen durch „Touch“

# Bedienkonzept Master



Aktivierete Funktionsmodule werden auf der Steuerleitung angezeigt

# Bedienkonzept Master



Funktionsmodule mit fehlenden Abhängigkeiten können nicht aktiviert werden

# Bedienkonzept Master



Konnektor HF-Gerät

Konnektor Nervmonitor

Konnektor Kamera

**Aktivierung nicht möglich**

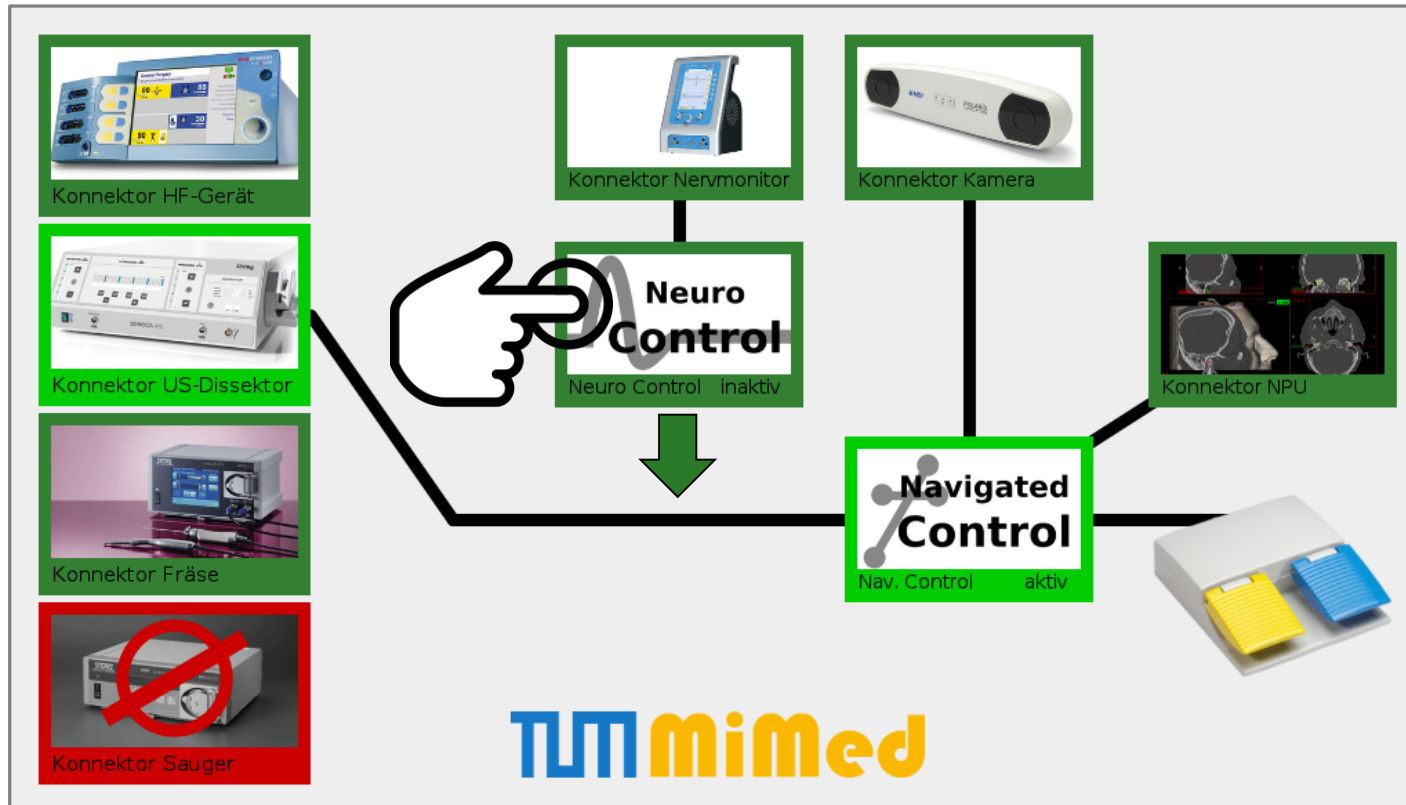
**Benötigtes Gerät fehlt:  
Konnektor Nervmonitor**

Konnektor Sauger

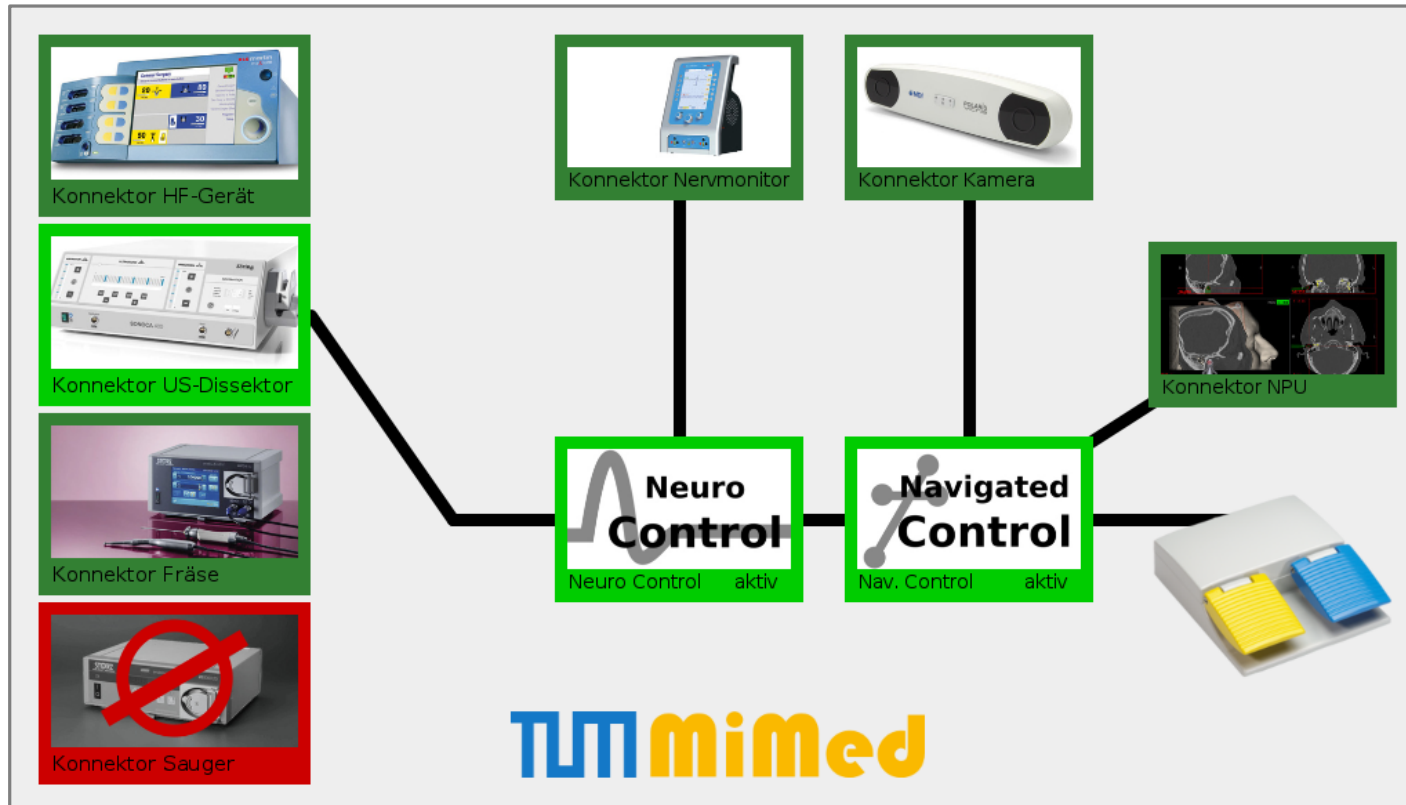
TUM mimed

Funktionsmodule mit fehlenden Abhängigkeiten können nicht aktiviert werden

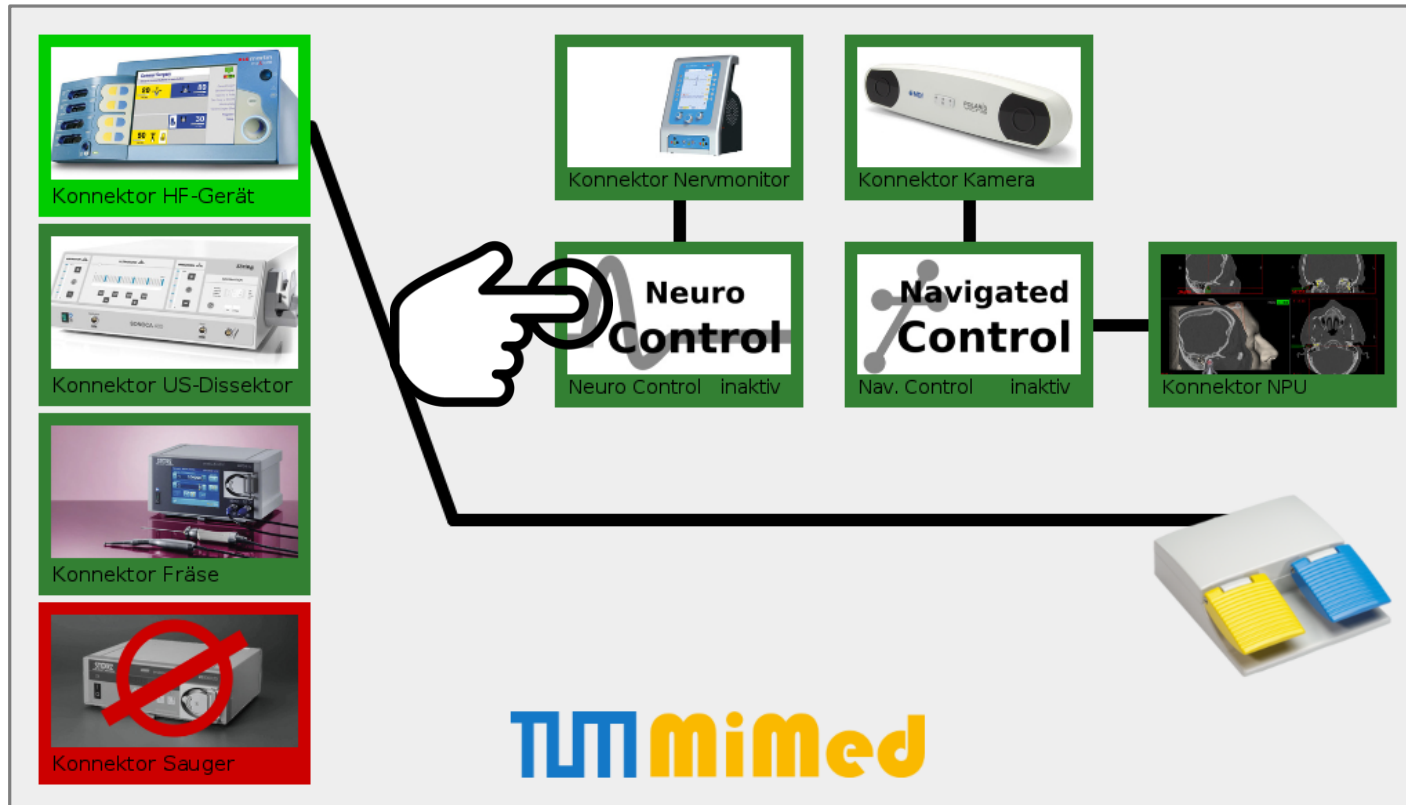
# Bedienkonzept Master



# Bedienkonzept Master



# Bedienkonzept Master



Funktionsmodule können nur mit kompatiblen Geräten eingesetzt werden



# Bedienkonzept Master

**Aktivierung nicht möglich**  
**Gesteuertes Gerät inkompatibel**

Konnektor HF-Gerät

Konnektor Nervmonitor

Konnektor Kamera

Konnektor Sauger

TUM mimed

Funktionsmodule können nur mit kompatiblen Geräten eingesetzt werden

# MiMed Echtzeitmaster

## Sicherheitsaspekte

# Sicherheitskonzept Master

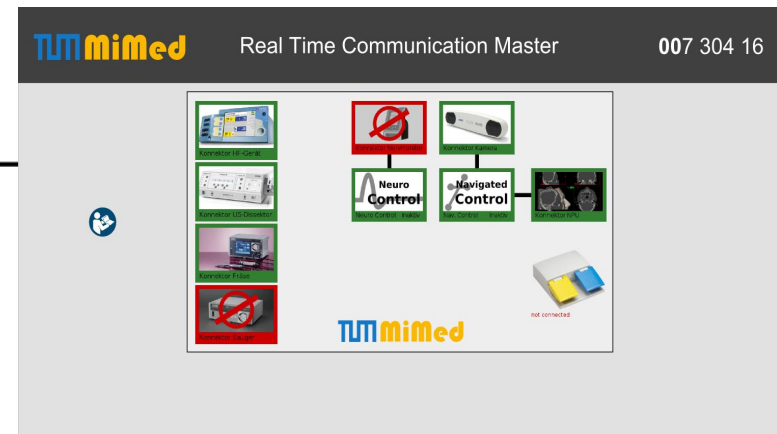
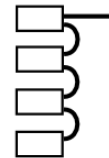
## Echtzeitmaster zentrale Komponente

Steuerung der Echtzeitkommunikation

Anbindung des Echtzeitnetzwerkes an OSCP

➤ Hohe Sicherheitsanforderungen

Echtzeit-  
Netz



OSCP  
Web  
KIS



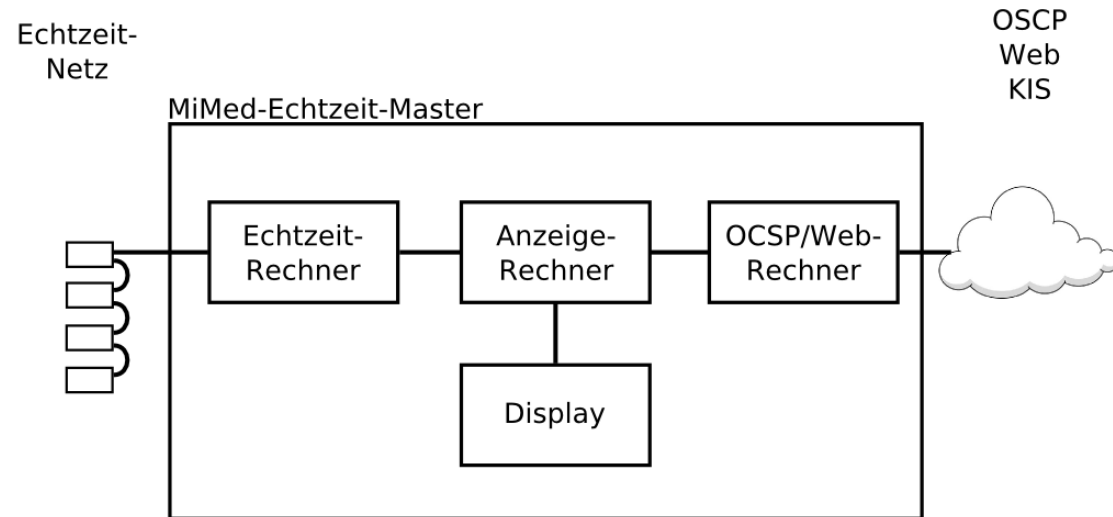
# Sicherheitskonzept Master

## Echtzeitmaster zentrale Komponente

Steuerung der Echtzeitkommunikation

Anbindung des Echtzeitnetzwerkes an OSCP

➤ Hohe Sicherheitsanforderungen



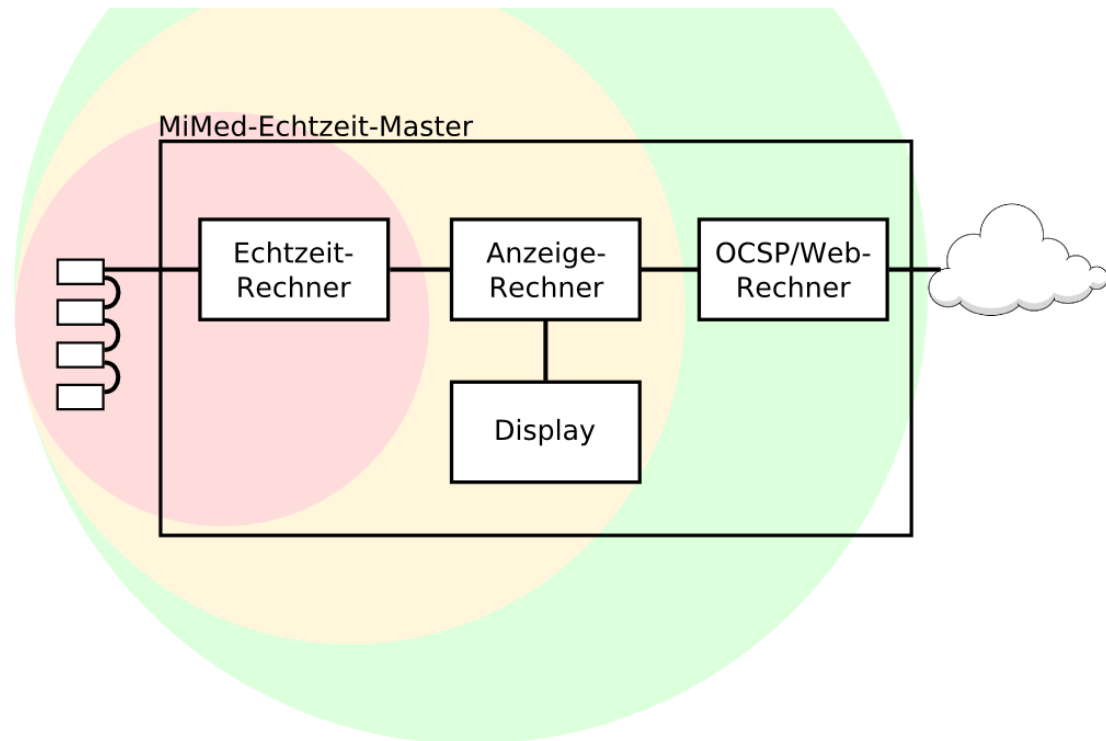
# Sicherheitskonzept Master

## 3-stufiger, zwiebelförmiger Aufbau

**Kern:** Echtzeitrechner

**Mittlere Schicht:** Steuerung Bedienpanel

**Äußere Schicht:** OSCP/Webschnittstelle

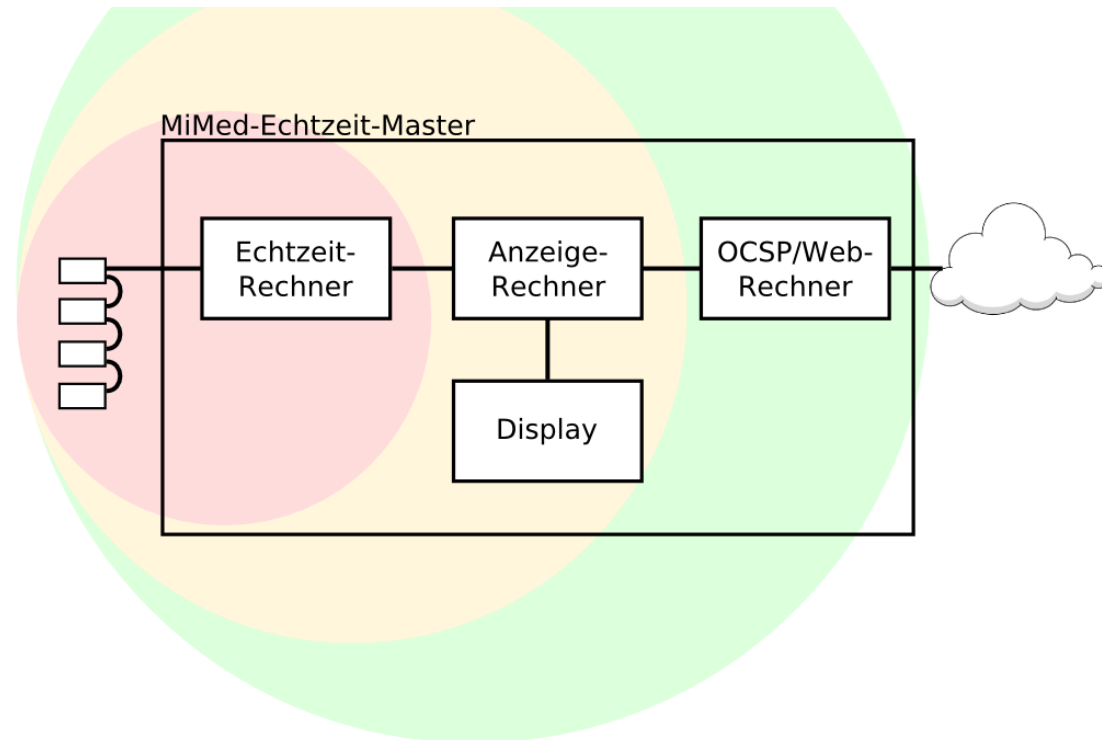


# Sicherheitskonzept Master

## Ausfallsicherheit

Kritische Komponenten funktionieren auch nach Ausfall der anderen

Kritischer Kern (Echtzeitrechner) kann redundant ausgelegt werden

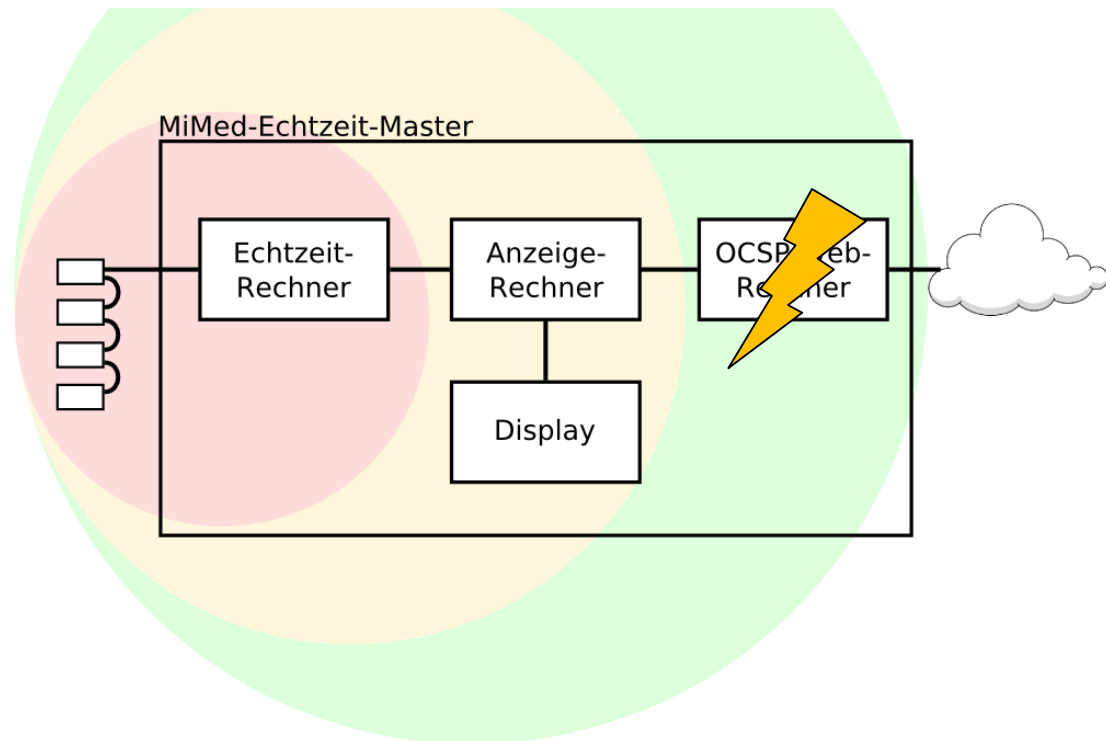


# Sicherheitskonzept Master

## Ausfallsicherheit

Kritische Komponenten funktionieren auch nach Ausfall der anderen

Kritischer Kern (Echtzeitrechner) kann redundant ausgelegt werden

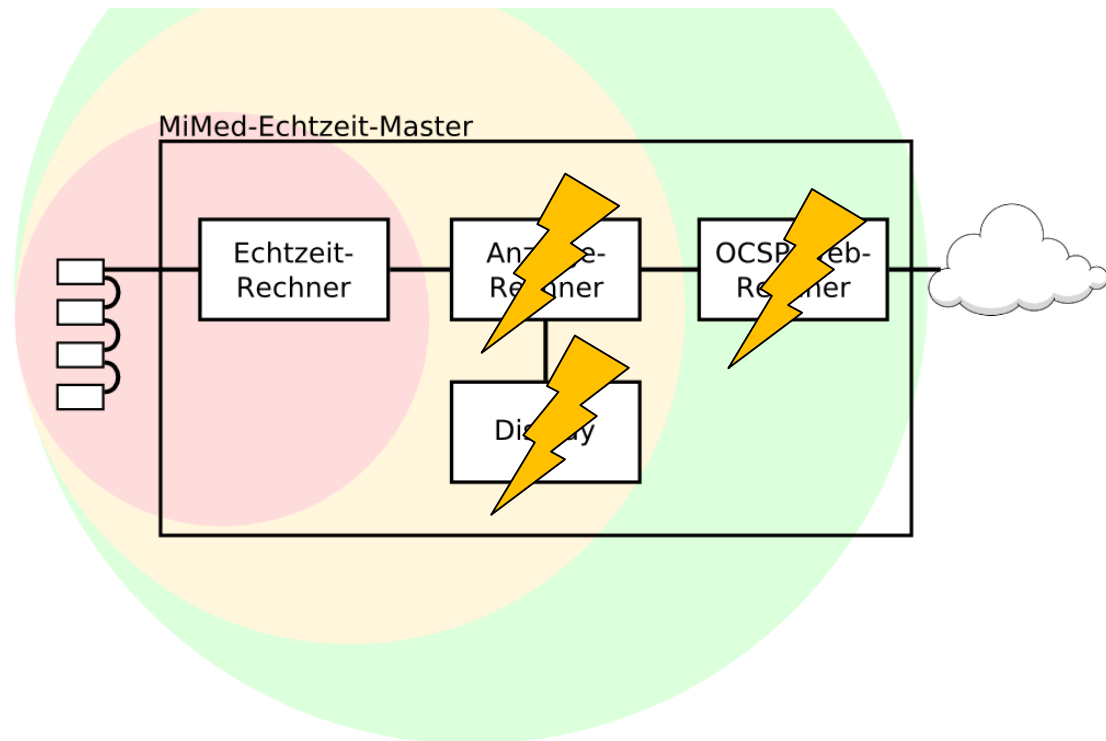


# Sicherheitskonzept Master

## Ausfallsicherheit

Kritische Komponenten funktionieren auch nach Ausfall der anderen

Kritischer Kern (Echtzeitrechner) kann redundant ausgelegt werden



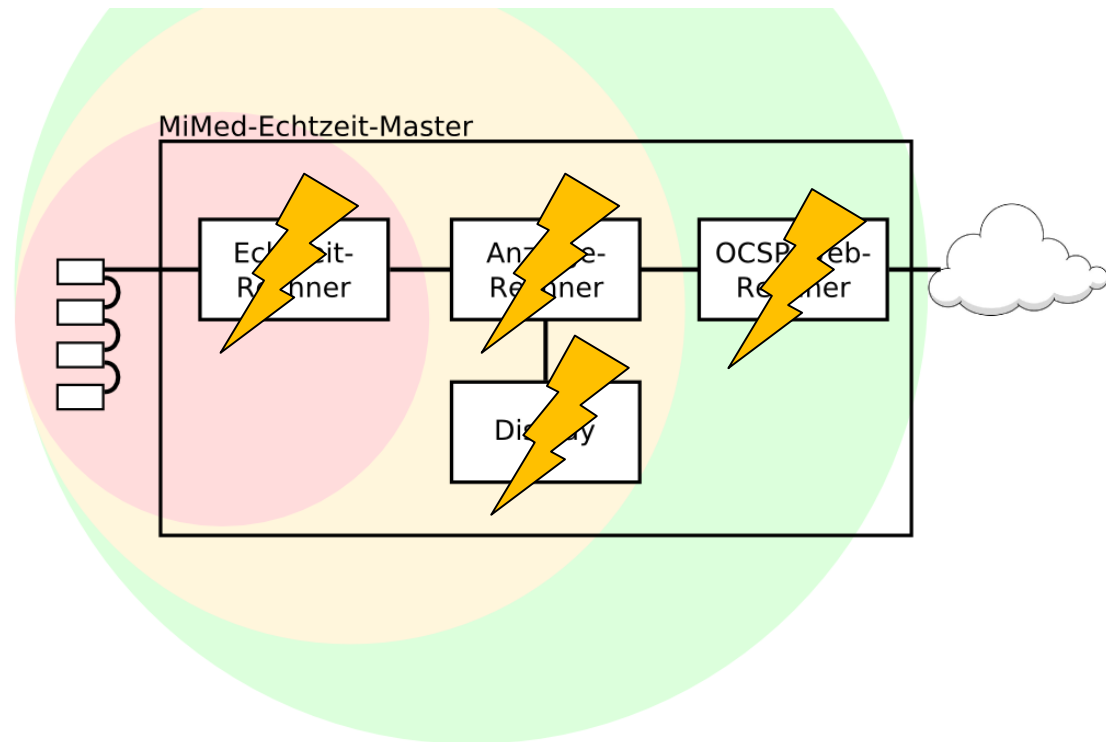


# Sicherheitskonzept Master

## Ausfallsicherheit

Kritische Komponenten funktionieren auch nach Ausfall der anderen

Kritischer Kern (Echtzeitrechner) kann redundant ausgelegt werden



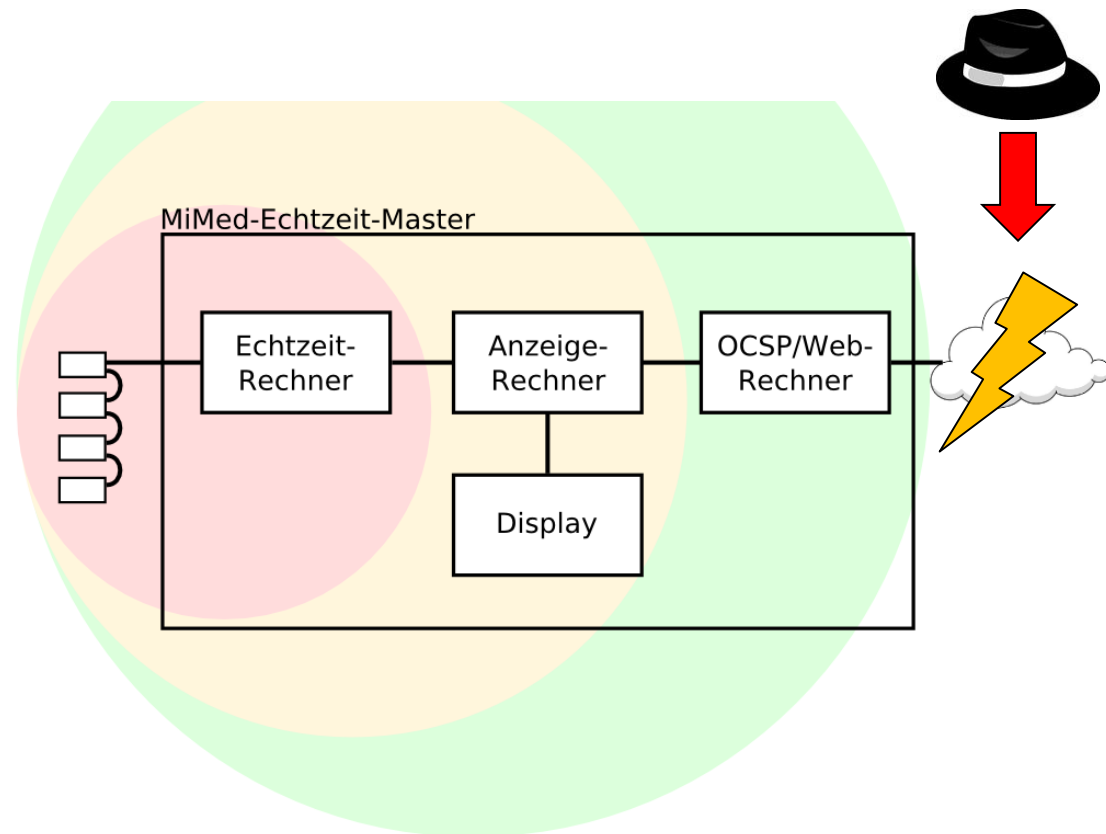
# Sicherheitskonzept Master

## Schutz vor DoS-Angriffen

Echtzeitnetz über drei Rechner isoliert

- Physikalischer Zugriff nötig

Keine Einschränkung kritischer Funktionalitäten auch bei erfolgreichem DoS gegen die OSCP/Web-Schnittstelle



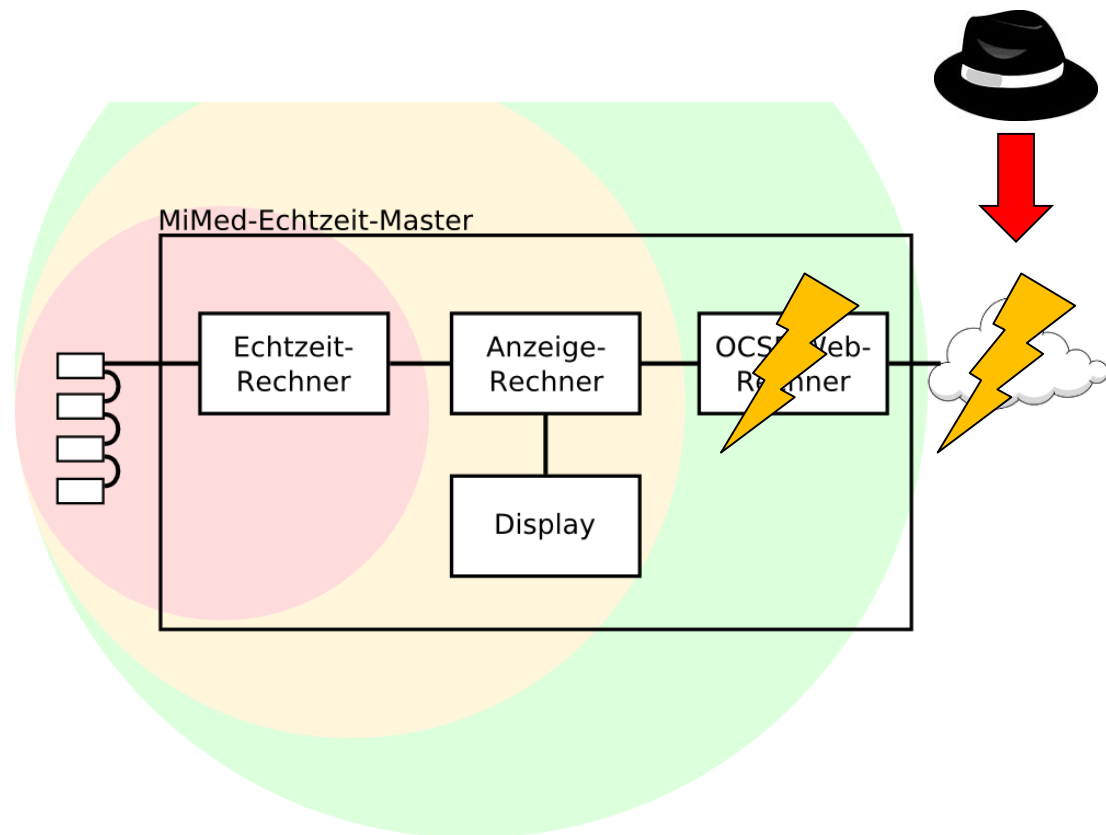
# Sicherheitskonzept Master

## Schutz vor DoS-Angriffen

Echtzeitnetz über drei Rechner isoliert

- Physikalischer Zugriff nötig

Keine Einschränkung kritischer Funktionalitäten auch bei erfolgreichem DoS gegen die OSCP/Web-Schnittstelle



**Vielen Dank für Ihre Aufmerksamkeit**

## Internes Protokoll

Getaktetes UDP

Master-Slave-Prinzip

- Keine Kollisionen, da nur zwei Teilnehmer pro Bus
- Deterministische Update-Intervalle
- Konstante Latenz (keine gefüllten Queues)
- Implizierendes Limitieren der Daten-/Befehlsrate
  - Schutz vor Überlastung (DoS)



**Echtzeit-Rechner**  
B&R X20



**Anzeige-Rechner**  
Raspberry Pi 2 Model B



**OSCP/Web-Rechner**  
Raspberry Pi 2 Model B