Universität Rostock

Traditio et Innovatio

Sicherheitsanalyse durch Entwicklung eines Rogue Device zur Echtzeitmanipulation maritimer Steuerungssysteme

Jakob Engelbert Tomahogh

Betreuer: *M.Sc. Marvin Davieds*
Zweitgutachter: *Prof. Dr. rer. nat. Clemens H. Cap*

14.02.2025

Motivation

- Sicherheit wurde in maritimen Systemen vernachlässigt
- Kommunikationssysteme sind anfällig für Angriffe
- Angriff auf Steuerungssysteme könnte katastrophale Folgen haben
- physischer Zugriff bei Passagierschiffen möglich

Zielsetzung

- Entwicklung eines Rogue Devices
- Anbindung an das Schiff über CAN-Bus und serielle Schnittstelle
- Eingabe der Befehle über einen Xbox Controller
- Übersetzung auf dem Rogue Device
- Steuerung des Schiffs

Zielsetzung

- Machbarkeit eines solchen Angriffs soll gezeigt werden
- Aufmerksamkeit auf Sicherheitslücken in maritimen Systemen lenken
- Sicherheitslücken sollen durch Steueurung mit Spielecontroller veranschaulicht werden

Schiffstechnik

Fig. 1: Forschungsschiff Limanda

- zweimotoriger Katermaran
- Länge: 15,73m
- Breite: 6,16m

Schiffstechnik

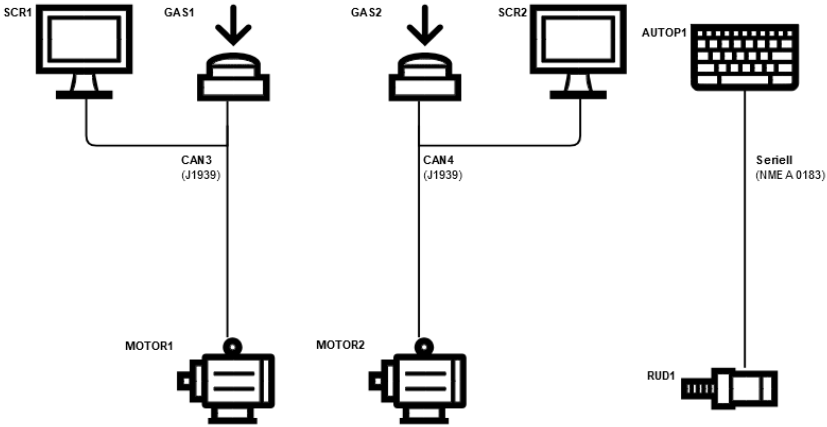

Fig. 2: Vereinfachter Aufbau des Systeme

CAN-Bus

- serielle Netzwerktechnologie, bei dem mehrere Geräte miteinander kommunizieren können
- ermöglichicht effiziente Kommunikation zwischen Steuergeräten
- alle Geräte sind gleichberechtigt
- Nachrichten werden nach Broadcast-Prinzip übertragen
- Kommunikation auf dem CAN-Bus ist unverschlüsselt

J1939

- Standard für die Kommunikation auf dem CAN-Bus
- Nutzt 29 Bit Extended CAN Identifier
- ermöglicht Knotenadressierung

CAN-Bus Nachricht

Fig. 3: Aufbau einer CAN-Bus Nachricht

- SOF: Start of Frame
- Arbitration Field: Nachrichten-ID und Remote Transmission Request
- Control Field: Datenlänge
- Data Field: Nutzdaten
- CRC Field: Prüfsumme
- EOF: End of Frame

- Entwicklung eines Rogue Devices
- Anbindung an das Schiff über den CAN-Bus
- Eingabe der Befehle über einen Xbox Series X Controller
- Übersetzung auf dem Rogue Device

- Anbindung des Raspberry Pi an den CAN-Bus
- Steuerung des Schiffes über den Controller

- Decodieren der CAN-Bus Nachrichten in Echtzeit
- Reagieren auf Gashebel Eingaben
- Testen der Steuerung
- Analyse der Auswirkungen
- Implementierung der Rudersteuerung