APEX connect 2018

Apex Integration in die Welt der Störmeldeanlagen und der Lichtsteuerung

PRAXISBERICHT GEBÄUDELEITTECHNIK MIT APEX - IOT MAL GANZ PRAKTISCH

GPI Consult

Gunther Pippèrr

http://www.pipperr.de - gunther@pipperr.de

Bergweg 14 - 37216 Witzenhausen/Roßbach

Freiberuflicher Oracle Datenbank Experte - Ich unterstütze Sie gerne in ihren Projekten.

Sparkassenakademie Bayern

Florian Aschenbrenner

Sparkassenakademie Bayern in Landshut

Die zentrale Bildungseinrichtung der Sparkassen-Finanzgruppe Bayern

https://www.sparkassenakademie-bayern.de

Der Veranstaltungsort für Ihr nächstes Seminar

Ausgangssituation

- Gebäudekomplex der Sparkassenakademie Bayern mit 70 Veranstaltungsräumen, 420 Hotelzimmern erbaut in den 80‘er Jahren
  - Zentrale Störmeldetechnik aus den 90'er Jahren
  - Zentrale Lichtsteuerung aus den 80'er Jahren
- Hohe Wartungs- und Softwarekosten für die veraltete Technologie
- Ersatzteil-Probleme mit zentralen Steuerkomponenten
- Komplex in der Anpassung auf neue Aufgaben in der Gebäudesteuerung

Projektziele „Zentrale Leittechnik“

- Zentrale Administration der Gebäudeleittechnik mit ~700 Störmeldesensoren
- Ertüchtigung der bisherigen Licht- und Gebäudesteuerung auf Basis einer VPS (Verbindungsprogrammierte Steuerung) durch ein speicherprogrammierbares Systems (SPS)
- Vollständige Integration in das bestehende IT-Monitoring (Paessler PRTG)
- Administration, Datenpflege und Dashboard-Ansichten der Umgebung in einer Oberfläche

Der eingesetzte Technologie Stack

- Gebäudetechnik
  - WAGO-Controller für die Steuerungs-/Signalisierungs-Aufgaben
  - Diverse ModbusTCP fähige Systeme (Heizung, Lüftung)

- TCP/IP Netzwerk
  - VLANs – Authentifizierung per IEEE 802.1X
  - ModbusTCP Protokoll – REST API

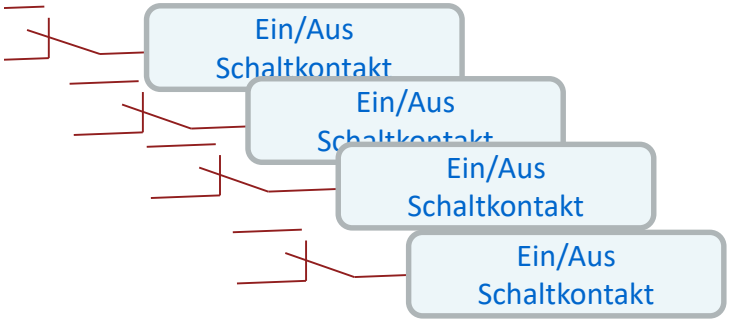
- Microsoft System Landschaft
  - Oracle 12c R2 Datenbank mit APEX 5.1
  - Microsoft Message Queue
  - IT-Monitoring (Paessler PRTG)

Das zentrale Konzept der Gebäudeleittechnik (1)

- Der WAGO-Controller
  - WAGO PFC100 und PFC200 Controller mit HTML5-Visualisierung und CODESYS3
  - Embedded-Linux basiert auf einem RT-Preempt-Realtime-Kernel. Ein Kernel mit einem Echtzeit-Patch
  - Implementierung in ST (Strukturierter Text) nach EN 61131-3
    - Sprache ist angelehnt an Pascal, steht folglich PL/SQL nahe

Das zentrale Konzept der Gebäudeleittechnik (2)

- Der WAGO-Controller
  - Zentrale Steuerung – zwei WAGO PFC200
  - dezentrale Komponenten
    - 25 WAGO PFC100 und 3 PFC200 Controller ersetzen die Alttechnik in den Gebäudeteilen



Warum APEX? (1)

- Oracle Technologie Erfahrung seit Ende der 90’er im Haus mit eigenen Mitarbeitern
  - Vollständig integriertes ERP Veranstaltungsmanagement der Akademie verwendet die Oracle Datenbank

- Mit Apex bereits erfolgreich Projekte umgesetzt
  - Akademie Kalender, Datenimport, Fundsachen ...

Warum APEX? (2)

- APEX überzeugt durch schnelle Einführung und fehlerfreie Implementierung im produktiven Einsatz

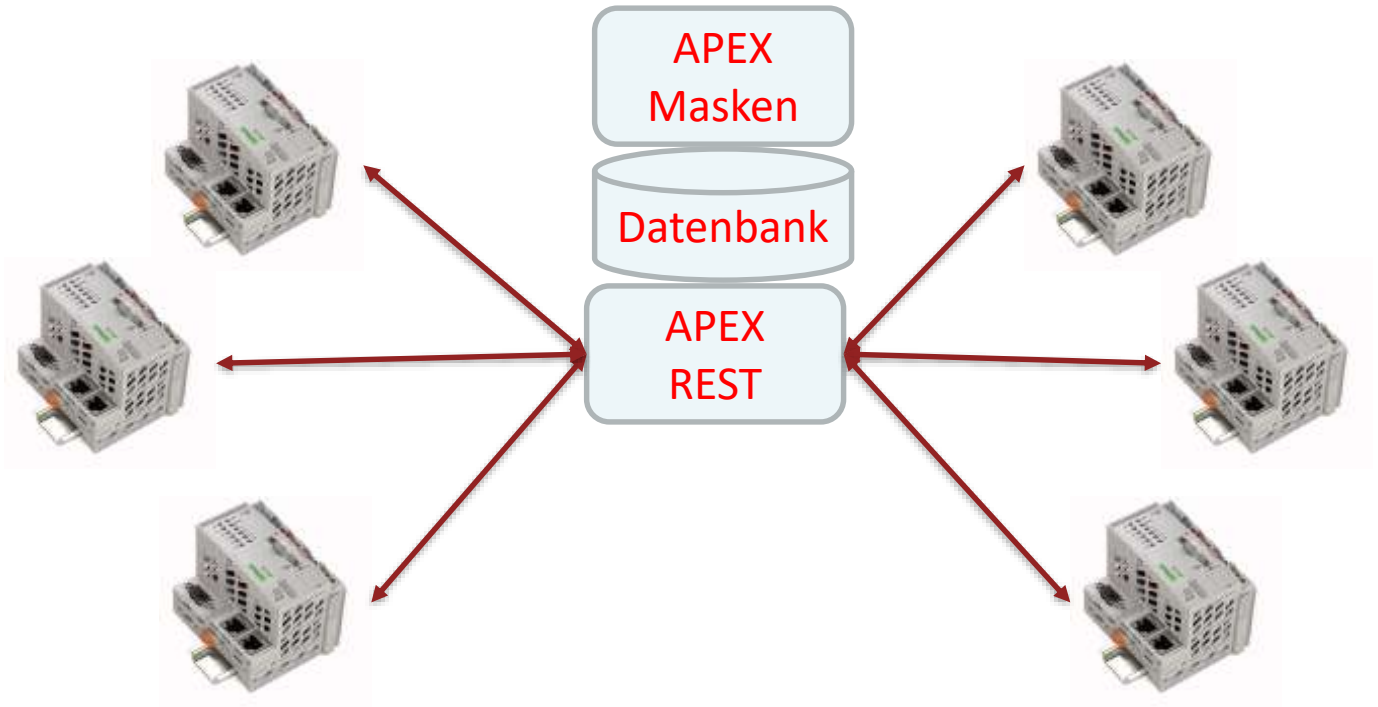
- Die Oracle Datenbank lässt sich auch unter Windows “einfach” in andere Welten integrieren
  - .Net Integration (External Procedure Feature)
  - PL/SQL API’s z.b. für LDAP Abfragen
  - REST Service

Die Aufgaben für APEX in diesem Verbund

- Zentrale Datenbank für das Logging von Störmeldungen
- Dashboard für Störmeldeanzeige bei Rezeption und Haustechnik
- Quittierung von neuen Meldungen um den Alarmierungsprozess am WAGO-Controller zu stoppen
- Zweite Bedienebene im Falle eines Ausfalls der GLT-Visualisierung für die wichtigsten Schaltpunkte
- Stammdaten-Pflege für die WAGO-Controller Störmeldekontakte und schaltbare Datenpunkte für Licht, Türen, Aufzüge, Rollladen usw.

Stammdaten Pflege für die WAGO Controller (1)

- “Software Konfiguration” über einen zentralen Punkt
  - Über APEX wird zentral die Konfiguration aller Controller gepflegt



In der GLT noch kein selbstverständliches Feature !

Stammdaten Pflege für die WAGO-Controller (2)

- Die Controller holen über REST API beim Start bzw. regelmäßig die für diesen Kontroller bestimmte Konfiguration
- Alle dezentral verteilten WAGO-Controller können mit dem selben CODESYS Programm betrieben werden

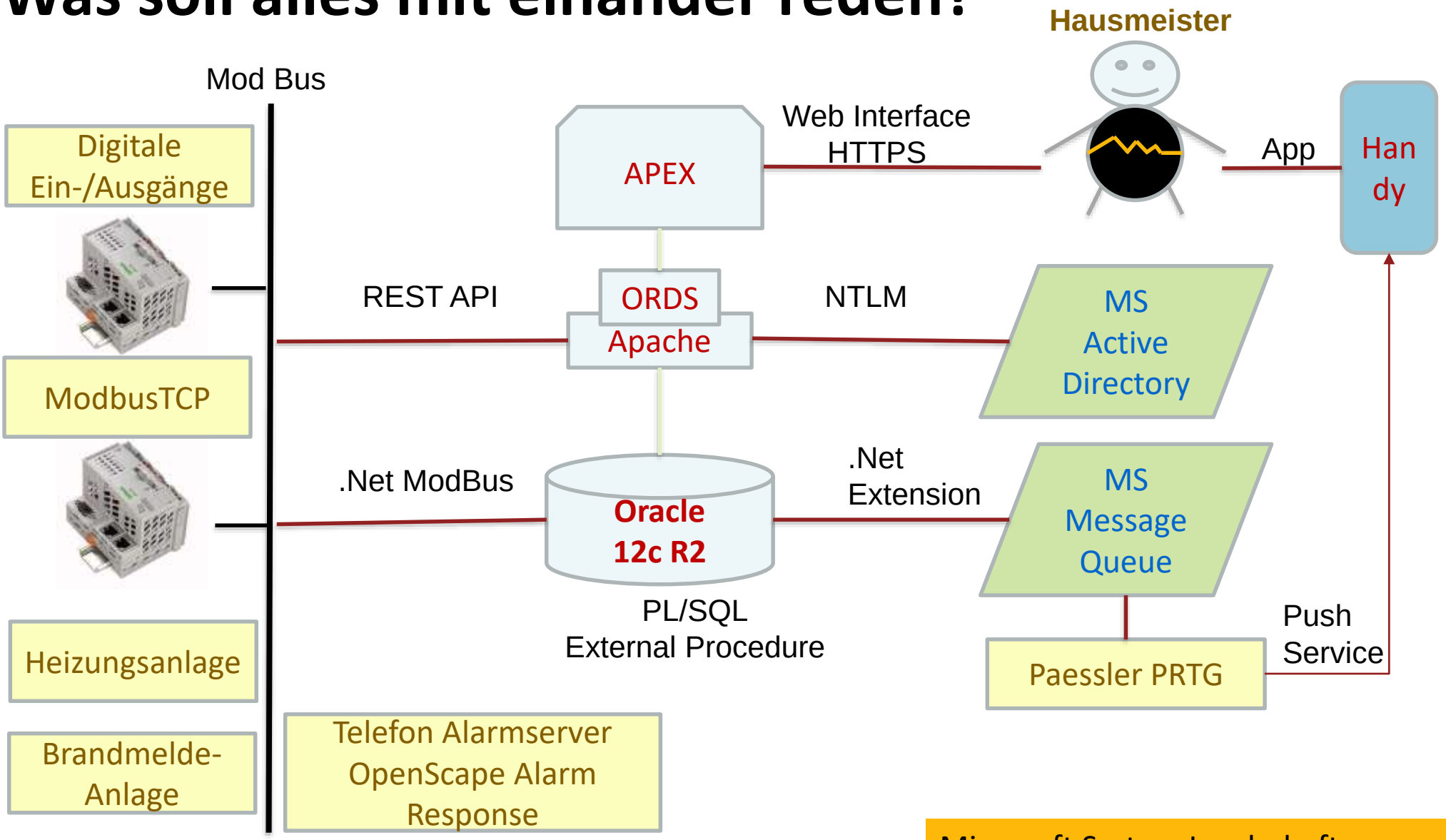
- D.h. der Elektriker kann einen defekten Controller mit einem Standby Gerät austauschen, kein Eingriff von einem Entwickler für die Konfiguration des Geräts notwendig!

Ermöglicht wartungsarmen 24/7 Betrieb auch bei Controller Ausfällen

Integration der WAGO Controller

- APEX RestWebservice JSON mit Basic http Auth
  - Übermittlung der Zustände von den WAGO-Controllern an APEX
    - Störmeldungen
    - System- und Alarmzustände
    - Logging
  - Abfrage der in Oracle gepflegten Stammdaten durch die WAGO-Controller

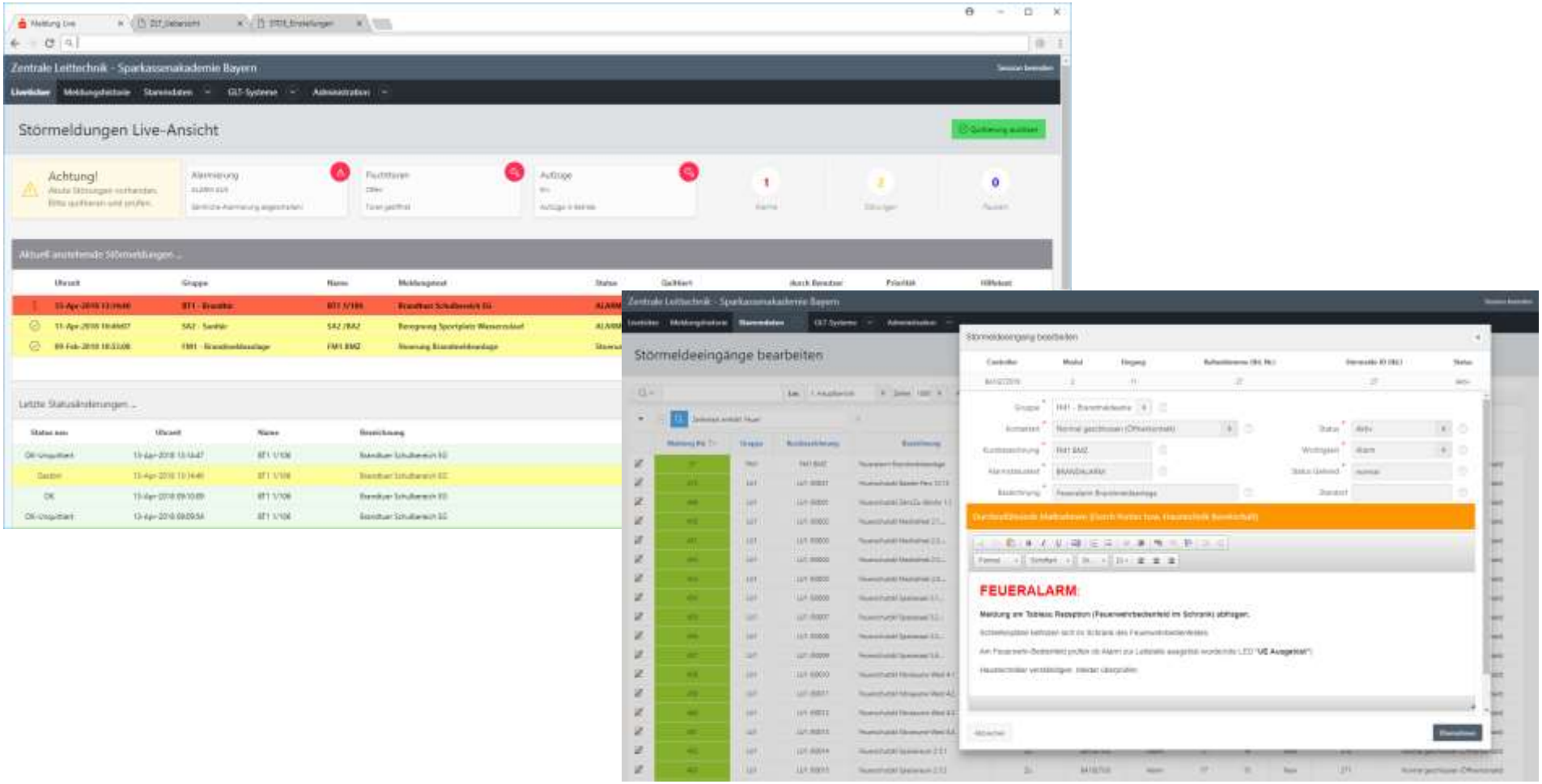
Was soll alles mit einander reden?



Microsoft System Landschaft

System Demonstration

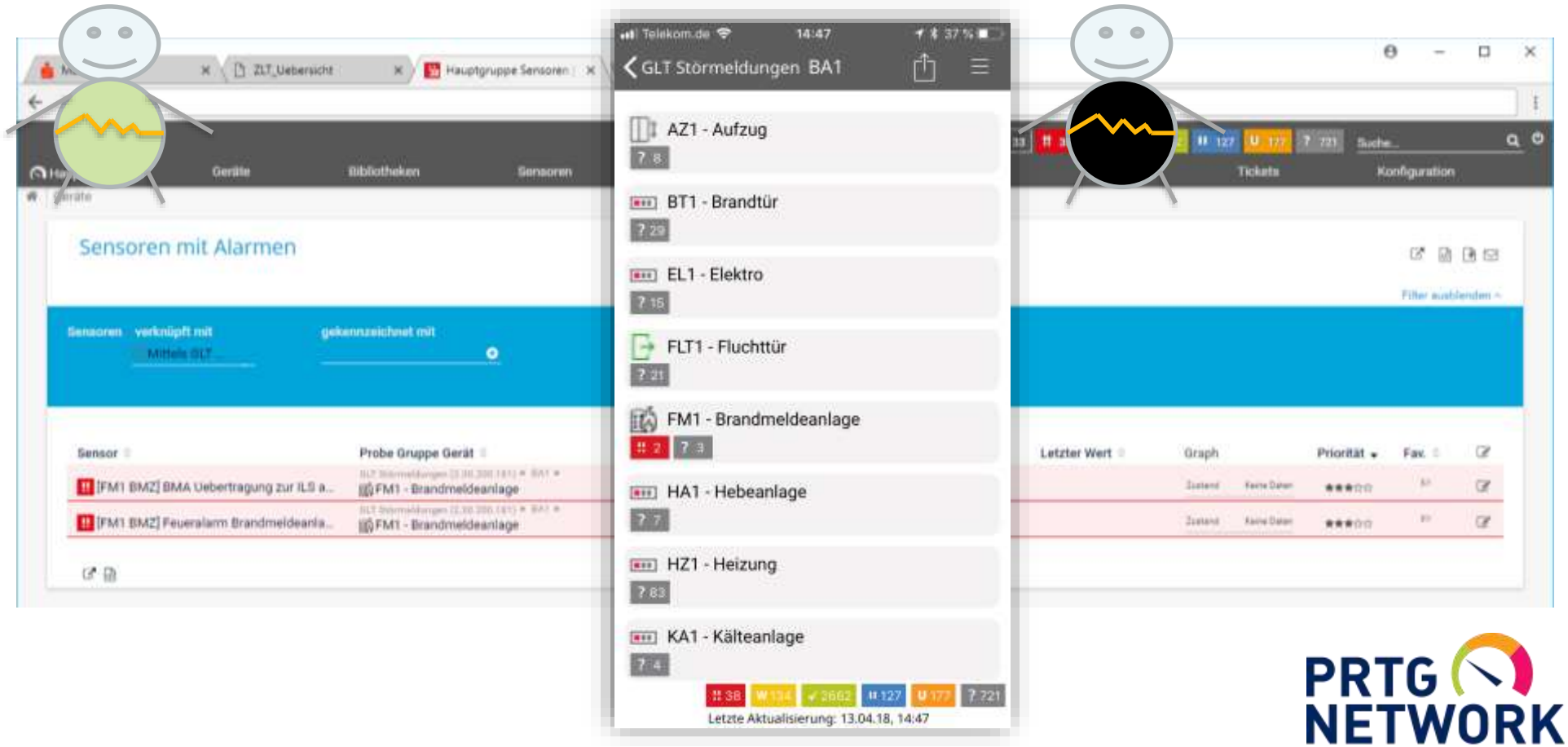
- Und so sieht das Ganze dann aus:



System Demonstration – Passler APP

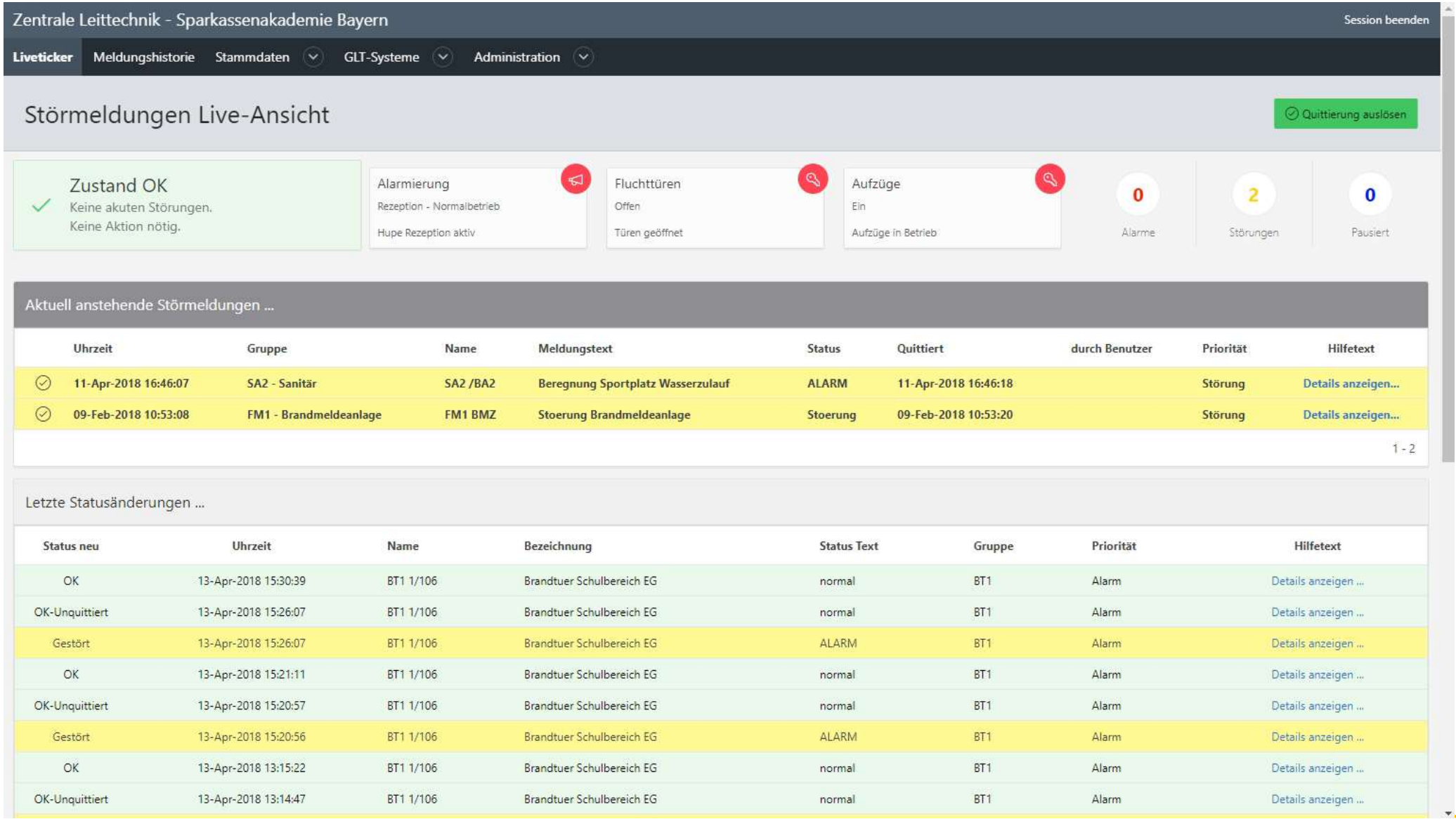
- Und so sieht das Ganze dann aus:

IT **Hausmeister**



PRTG NETWORK MONITOR

Demo

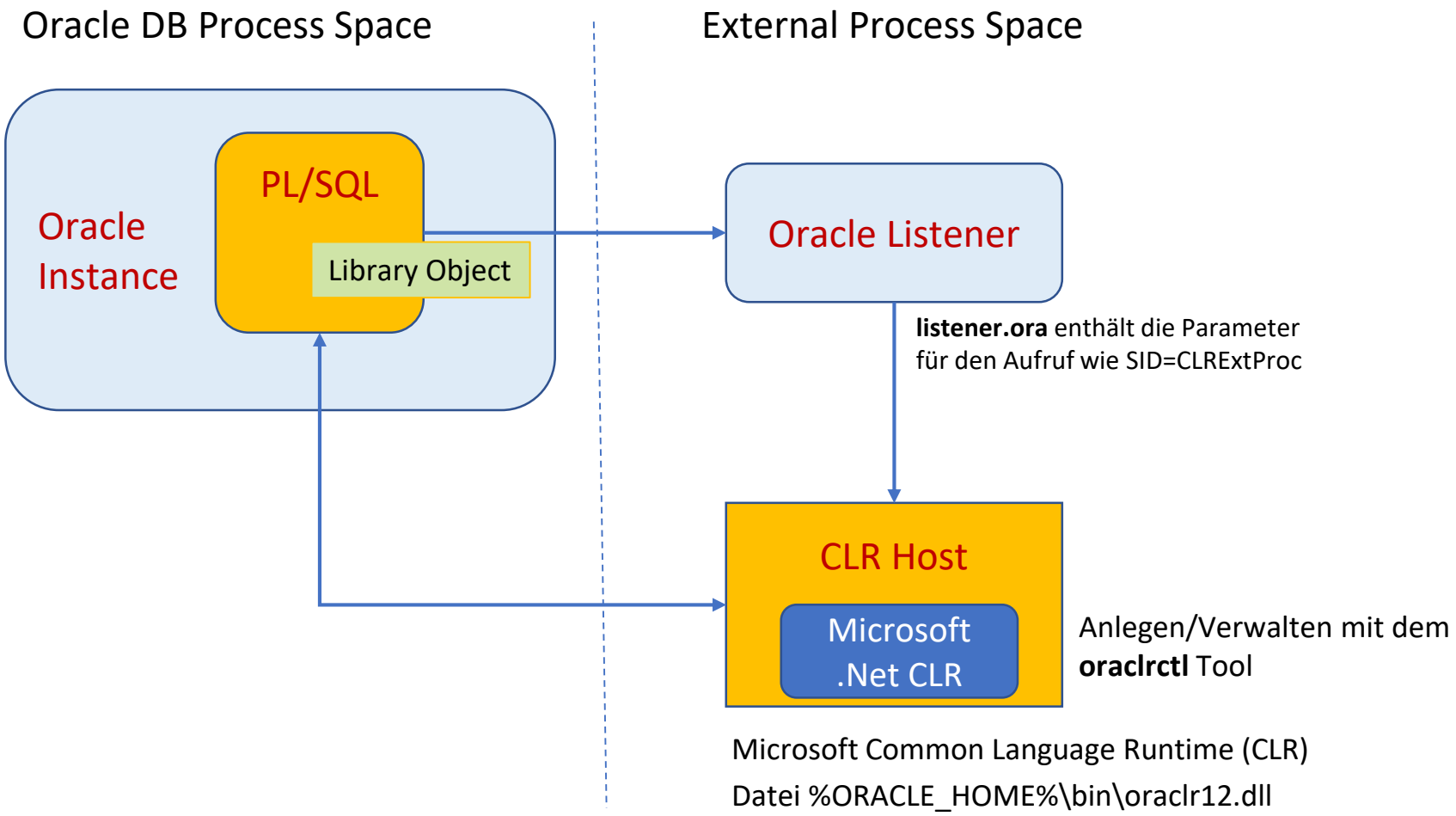

Zentrale Leittechnik - Sparkassenakademie Bayern
Session beenden
Liveticker
Meldungshistorie
Stammdaten
GLT-Systeme
Administration
Störmeldungen Live-Ansicht
Quittierung auslösen
Zustand OK
Keine akuten Störungen.
Keine Aktion nötig.
Alarmierung
Rezeption - Normalbetrieb
Hupe Rezeption aktiv
Fluchttüren
Offen
Türen geöffnet
Aufzüge
Ein
Aufzüge in Betrieb
0
Alarme
2
Störungen
0
Pausiert
Aktuell anstehende Störmeldungen ...
Uhrzeit
Gruppe
Name
Meldungstext
Status
Quittiert
durch Benutzer
Priorität
Hilfetext
11-Apr-2018 16:46:07
SA2 - Sanitär
SA2 /BA2
Beregnung Sportplatz Wasserzulauf
ALARM
11-Apr-2018 16:46:18
Störung
Details anzeigen...
09-Feb-2018 10:53:08
FM1 - Brandmeldeanlage
FM1 BMZ
Stoerung Brandmeldeanlage
Stoerung
09-Feb-2018 10:53:20
Störung
Details anzeigen...
1 - 2
Letzte Statusänderungen ...
Status neu
Uhrzeit
Name
Bezeichnung
Status Text
Gruppe
Priorität
Hilfetext
OK
13-Apr-2018 15:30:39
BT1 1/106
Brandtuer Schulbereich EG
normal
BT1
Alarm
Details anzeigen ...
OK-Unquittiert
13-Apr-2018 15:26:07
BT1 1/106
Brandtuer Schulbereich EG
normal
BT1
Alarm
Details anzeigen ...
Gestört
13-Apr-2018 15:26:07
BT1 1/106
Brandtuer Schulbereich EG
ALARM
BT1
Alarm
Details anzeigen ...
OK
13-Apr-2018 15:21:11
BT1 1/106
Brandtuer Schulbereich EG
normal
BT1
Alarm
Details anzeigen ...
OK-Unquittiert
13-Apr-2018 15:20:57
BT1 1/106
Brandtuer Schulbereich EG
normal
BT1
Alarm
Details anzeigen ...
Gestört
13-Apr-2018 15:20:56
BT1 1/106
Brandtuer Schulbereich EG
ALARM
BT1
Alarm
Details anzeigen ...
OK
13-Apr-2018 13:15:22
BT1 1/106
Brandtuer Schulbereich EG
normal
BT1
Alarm
Details anzeigen ...
OK-Unquittiert
13-Apr-2018 13:14:47
BT1 1/106
Brandtuer Schulbereich EG
normal
BT1
Alarm
Details anzeigen ...

Umsetzung – Anbindung Oracle DB an .Net (1)

- Verwendung des external Procedure Features der DB
  - Lizenzkostenfrei verwendbar in allen Editionen

- Über .Net Klassen erfolgt die Integration
  - MS Message Queue
  - ModbusTCP
    - NET Modbus-Library => EasyModbus http://easymodbustcp.net/de/

Übersicht .Net Integration



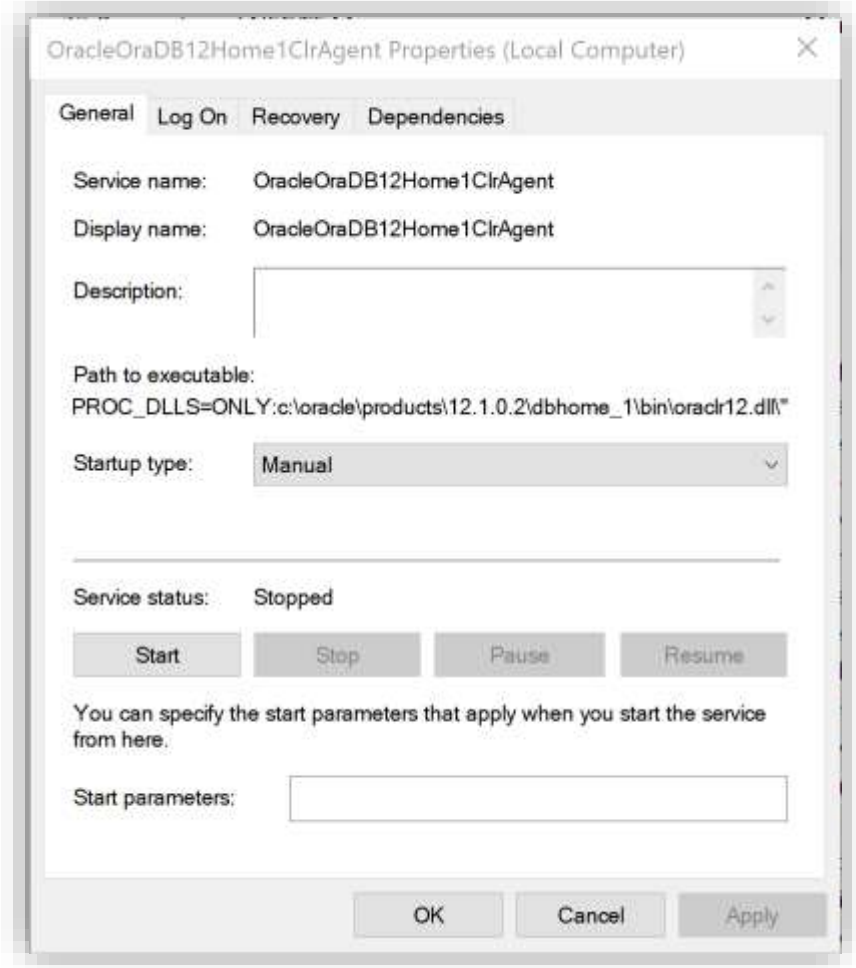
Prinzipieller Ablauf

- Funktionalität des Oracle Wizard in VS Studio nützen!
- Setup Umgebung
  - .Net Oracle Library auf DB Maschine deployen
  - SQL*Net Settings für Oracle Listener erstellen
  - CLR Service anlegen und starten
- Implementierung der eigenen Lösung
  - .Net DLL erstellen
  - DLL nach $ORACLE_HOME/bin/clr kopieren
  - PL/SQL Wrapper über das DBMS_CLR erstellen
  - Aufruf über PL/SQL

Im Detail https://www.pipperr.de/dokuwiki/doku.php?id=prog:windows_dot_net_integration_plsql

CLR Service unter MS Windows anlegen

Microsoft Common Language Runtime (CLR)



Läuft unter dem Oracle DB runner Owner!

Anlegen mit:

- **Oracle Database Extensions for .NET in der Datenbank aktivieren**
  - `chopt enable ode_net`
- **Oracle CLR Host Service anlegen**
  - `oraclrctl -new`

Erzeugt den folgenden Service:

```
c:\oracle\products\12.1.0.2\dbhome_1\bin\OraClrAgnt.exe agent_sid=CLRExtProc
max_dispatchers=2 tcp_dispatchers=0
max_task_threads=6 max_sessions=25
ENVS=\"EXTPROC_DLLS=ONLY:c:\oracle\products\12.1.0.2\dbhome_1\bin\oraclr12.dll\"
```

Konfiguration listener/tnsnames.ora

Oracle Instance

tnsnames.ora

Oracle Listener

Listener.ora

```
ORACLR_CONNECTION_DATA =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = IPC)(KEY = EXTPROC1))
    )
    (CONNECT_DATA =
      (SID = CLRExtProc)
      (PRESENTATION = RO)
    )
  )

EXTPROC_CONNECTION_DATA =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = IPC)(KEY = EXTPROC1))
    )
    (CONNECT_DATA =
      (SID = PLSExtProc)
      (PRESENTATION = RO)
    )
)
```

```
SID_LIST_LISTENER =
  (SID_LIST =
    (SID_DESC =
      (SID_NAME = CLRExtProc)
      (ORACLE_HOME = C:\oracle\products\12.1.0.2\dbhome_1)
      (PROGRAM = extproc)
      (ENVS = "EXTPROC_DLLS=ONLY:C:\oracle\products\12.1.0.2\dbhome_1\bin\oraclr12.dll")
    )
    (SID_DESC =
      (SID_NAME = PLSExtProc)
      (ORACLE_HOME = D:\oracle\product\12.1.0.2\dbhome_1)
      (PROGRAM = extproc)
    )
    (SID_DESC =
      (GLOBAL_DBNAME = GPI)
      (ORACLE_HOME = C:\oracle\products\12.1.0.2\dbhome_1)
      (SID_NAME = GPI)
    )
  )

LISTENER=
  (DESCRIPTION_LIST =
    (DESCRIPTION =
      (ADDRESS = (PROTOCOL = TCP)(HOST = 10.10.10.1)(PORT = 1521))
      (ADDRESS = (PROTOCOL = TCPS)(HOST = 10.10.10.1)(PORT = 2484))
      (ADDRESS = (PROTOCOL = IPC)(KEY = EXTPROC1))
    )
  )
```

Auf die richtige TNSNames achten!
Im Cluster die vom Grid User!

Anbindung DB an .Net - Probleme

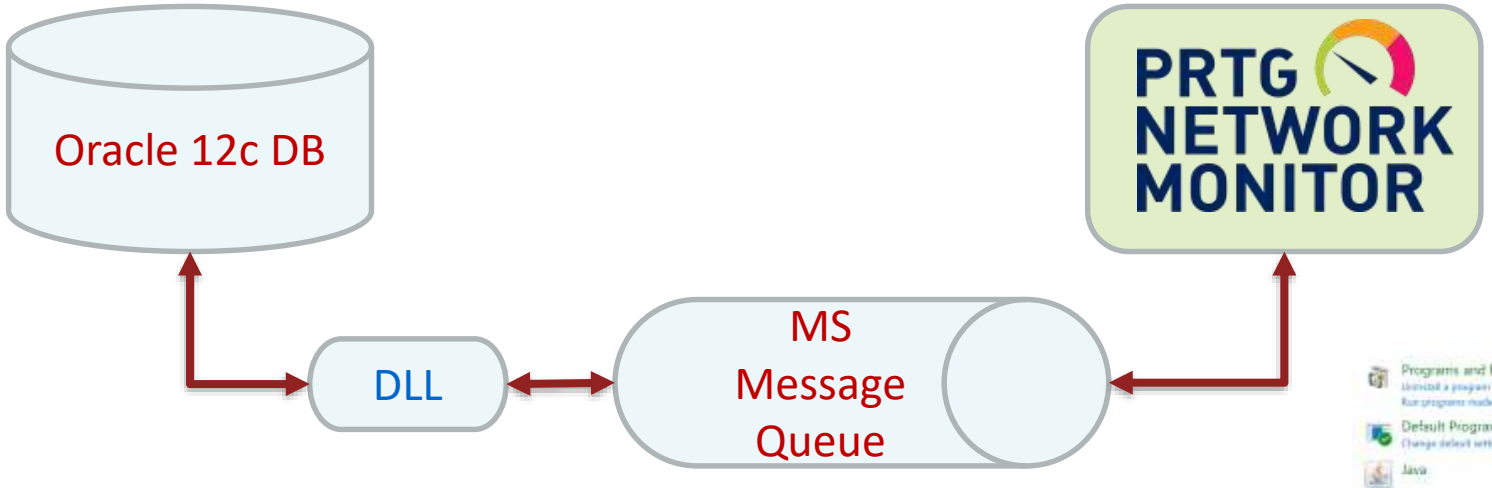
- Zugriff auf DLL der Oracle-DB verhindert Deployment!
  - Wird die eigene Library daher durch ständiges Pollen im 24/7 Betrieb geblockt kann das Deployment ein Problem darstellen! (gelöst durch umstellen auf REST API)

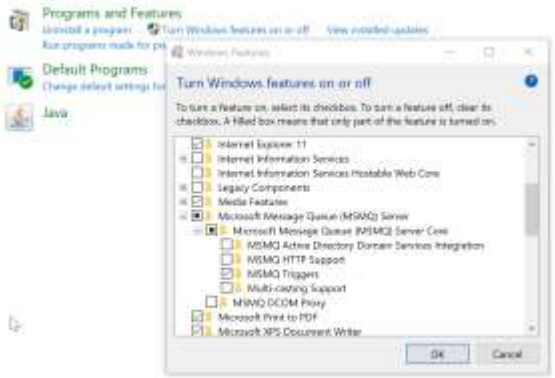
- Bei jeden Patch müssen die Libraries des external procedure Stack für .Net manuell neu auf dem Sever ausgerollt werden!

- Visual Studio Deployment als SYS in der DB, nur mit VS Assistenten – nicht mit Skript möglich
  - Unpraktisch für größere, gehostete Umgebungen

Zugriff auf MS Message Queue

- Über .Net kann nun auf alles notwendige Zugriffen werden



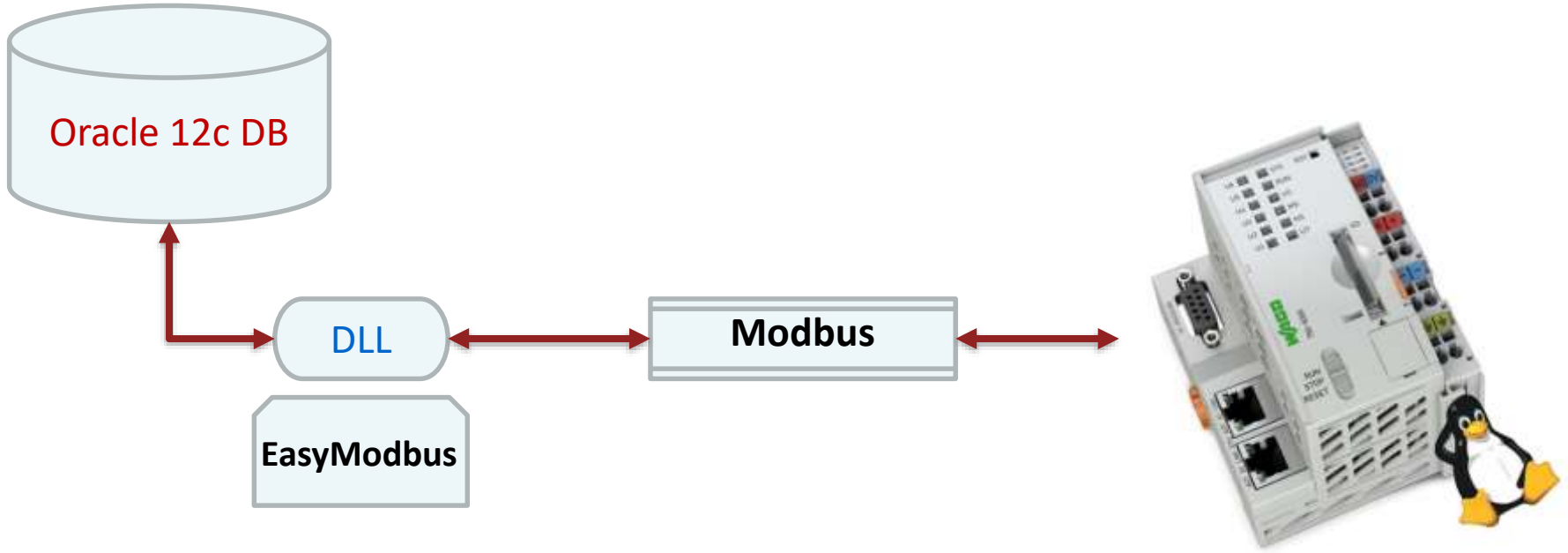


Warum die MS Message Queue verwenden?
Lizenzkostenfrei, Standard Windows Server und Client Feature

Vorteil:
MS Message Queue ist transaktional

ModbusTCP Zugriff

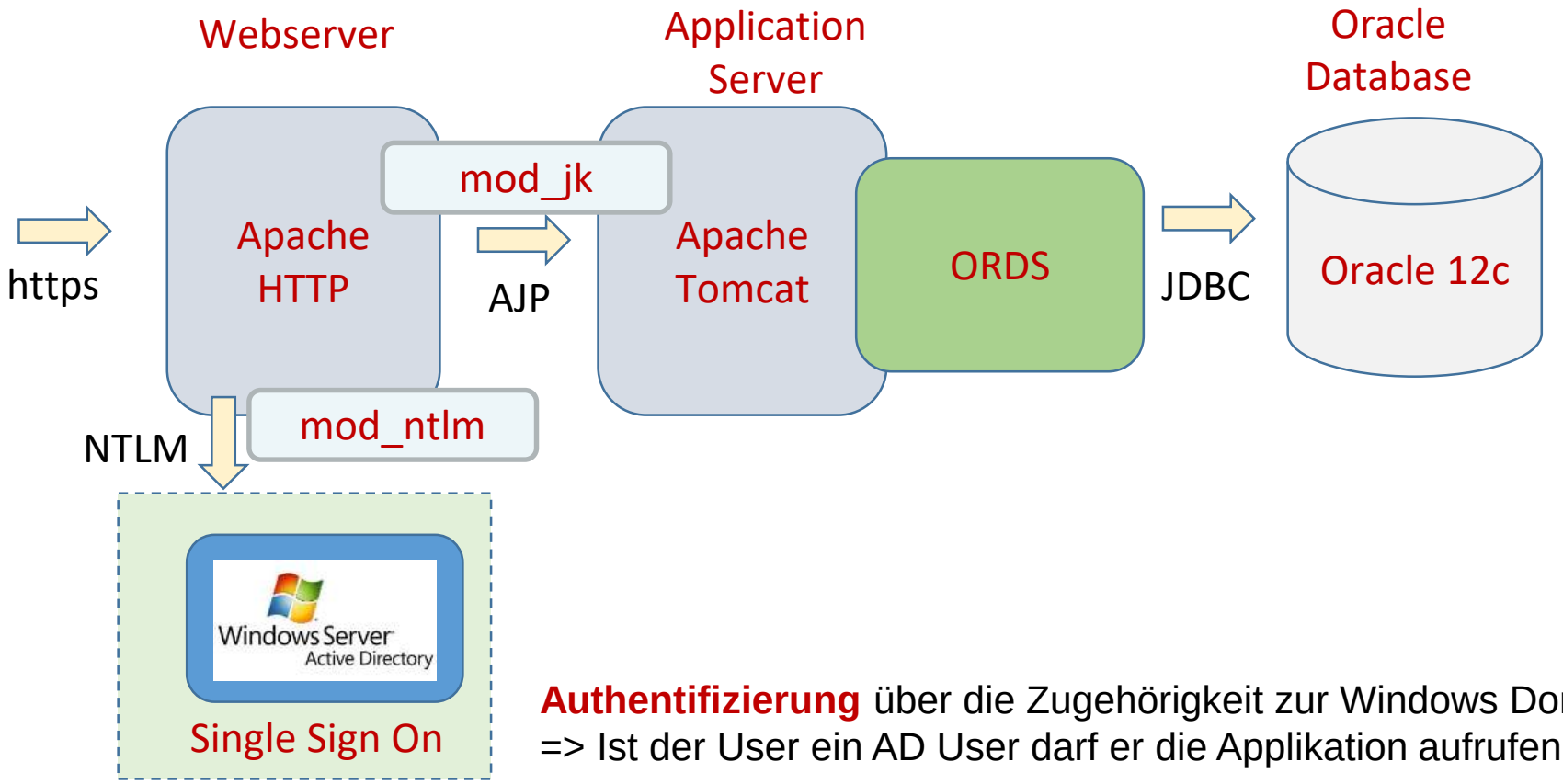
- Über eigene .NET C# DLL auf Basis von EasyModbus



Siehe => http://easymodbustcp.net/en/

APEX Integration mit mod_ntlm und mod_jk

- Da 100% Windows Umgebung mit NTLM umgesetzt



Authentifizierung über die Zugehörigkeit zur Windows Domain
=> Ist der User ein AD User darf er die Applikation aufrufen!

Details https://www.pipperr.de/dokuwiki/doku.php?id=prog:oracle_rest_data_service_tomcat
Für Kerberos Integration siehe Niels de Bruijn => Single Sign-On for APEX applications based on Kerberos

Authentisierung – Authorisierung

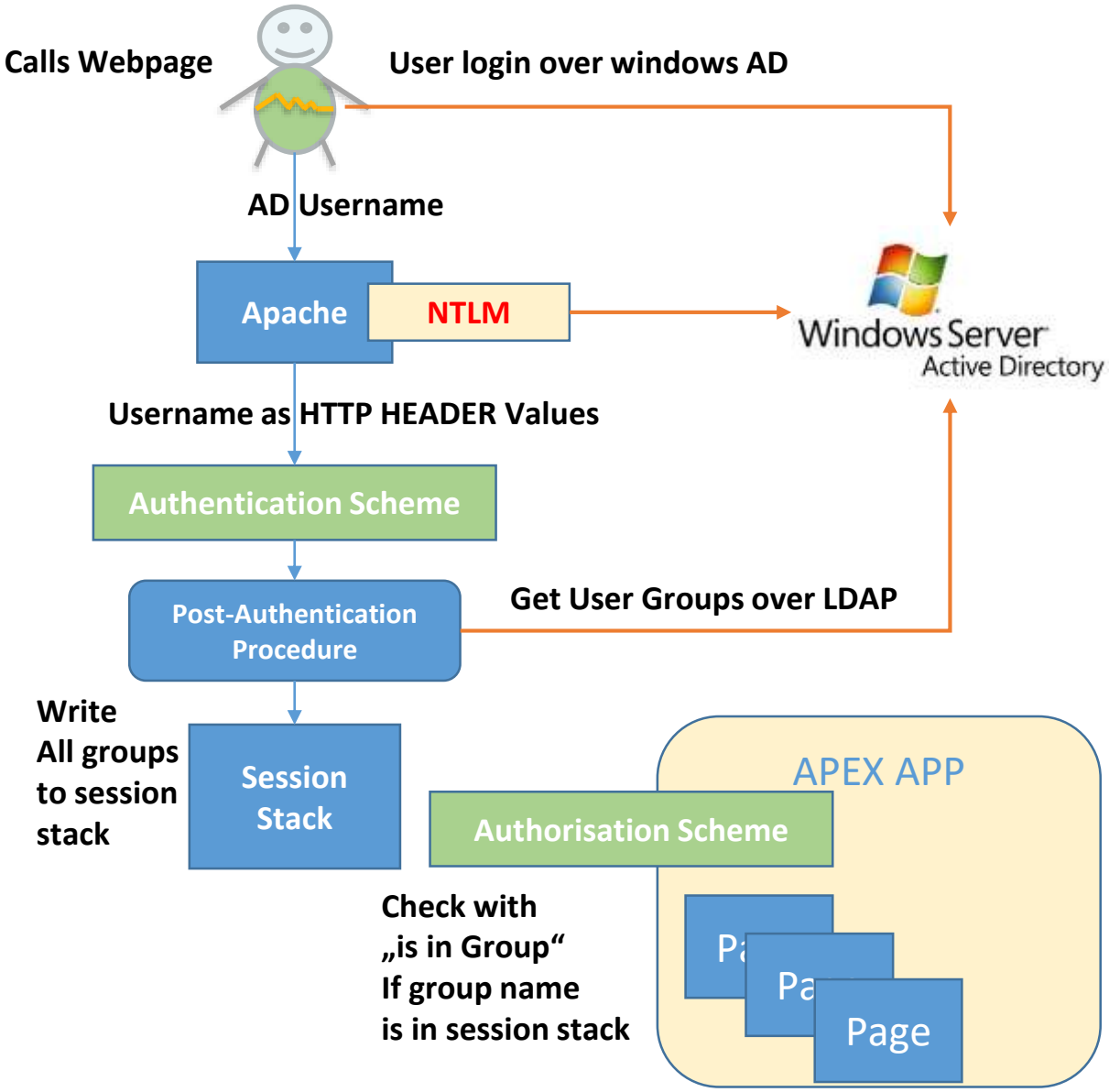
Authentication Scheme

Authentifizierung
über die Zugehörigkeit
zur Windows Domain
⇒ Ist der User ein AD User
darf er die Applikation aufrufen!

Authorisation Scheme

Authorisierung
über die Zugehörigkeit
zu einer Rolle im AD

⇒ Hat der User eine bestimmte
Rolle darf der User ein Element
in APEX sehen/öffnen!



DBMS_LDAP für die Abfrage des AD verwenden

```
  v_retval := DBMS_LDAP.search_s(ld => p_session
                                , base => g_ldap_base
                                , scope => DBMS_LDAP.scope_subtree
                                , filter => g_ad_user_type||p_username
                                , attrs => v_attrs
                                , attronly => 0
                                , res => v_message
                                );
<< entry_loop >>
WHILE v_entry IS NOT NULL
LOOP
  -- Get all the attributes for this entry.
  DBMS_OUTPUT.put_line('-----------------------------------');
  v_attr_name := DBMS_LDAP.first_attribute(ld => p_session, ldapentry => v_entry, ber_elem => v_ber_element);
  << attributes_loop >>
  WHILE v_attr_name IS NOT NULL
  LOOP
    -- Get all the values for this attribute.
    v_vals := DBMS_LDAP.get_values (ld => p_session
                                , ldapentry => v_entry
                                , attr => v_attr_name);
    BEGIN
      << values_loop >>
      FOR i IN v_vals.FIRST .. v_vals.LAST
      LOOP
```

LDAP Baum auslesen

Nachteil: Feste IP/Name des Domain Controllers notwendig, Domain kann nicht abstrakt hinterlegt werden und das Password eines Domainusers muss irgendwo hinterlegt werden!

Details unter => https://www.pipperr.de/dokuwiki/doku.php?id=prog:oracle_apex_active_directory_integration

Umsetzung – APEX AD Integration mit C#

- Synchronisierung von Benutzer und Gruppen aus den AD in die Oracle Datenbank letztendlich dann doch mit C# gelöst

  – Mit .NET-Objekten bessere Integration in der Windows Welt beim Zugriff auf das Active Directory
    - Wie Verwendung der Domain Names (nicht den DC Server!)
    - Auflösen der Gruppen Zuordnung eines Accounts (rekursiv)

  – Eingesetzt wurde hierfür folgende .NET API: **`System.DirectoryServices.AccountManagement-Namespace`**

Anbindung über REST Data Service

- APEX REST Listener im Einsatz
  - Verknüpfung alle Komponenten über das HTTP Protokoll
  - Der Standard für die „lockere“ Kopplung von Komponenten aus verschiedenen Welten
  - Warum APEX REST Services und nicht ORDS
    - Integration in der APEX Oberfläche hilfreich beim schnellen Einsatz des Features

mit dem **RE**presentational **S**tate **T**ransfer (abgekürzt REST)
wird ein Programmierparadigma für verteilte Systeme bezeichnet,
das insbesondere für Webservices verwendet wird.

Siehe auch
https://www.pipperr.de/dokuwiki/doku.php?id=prog:first_steps_oracle_rest_data_service

Security – Wichtige Maßnahmen

- Active Directory Integration der Anwender in APEX (Kennung und Rollenkonzept)
- Härten der WAGO Controller; Wie:
  - WAGO Firewall erlaubt nur DB Server IP für Modbus Zugriff
  - Verwendung von SSL (HTTPS) für die HTTP Kommunikation
  - Abschalten aller unnötigen Ports etc.
  - Dediziertes VLAN für die Gebäudeleittechnik
- Modbus Security
  - Erst im Aufbau Siehe => https://www.cyberbit.com/scada-modbus-protocol-vulnerabilities/

Sicherheit ist ein integrale Bestandteil einer jeden IOT Architekur!

Cloud Überlegungen im Projekt

- Was sprach gegen eine Cloud Lösung?
  - Die direkte Koppelung von APEX mit dem ERP System in der gleichen Datenbank ermöglicht eine sehr tiefe Integration.
  - Netzwerk – Lokal einfacher zu integrieren in die eigene Umgebung
  - Implementierung mit reinen REST API Lösung zwar möglich aber in Summe zu aufwendig

- Aber – Diese Cloud Lösung ist im Projekt im Einsatz
  - Die Source Code Verwaltung erfolgt mit Microsoft Visual Studio Team Services

Unsere nächsten Ziele

- Node.js, um nicht mehr mit dem Dashboard permanent zu pollen
  - Siehe Artikel im Red Stack Magazin 05/2017 von André Borngräber
- Nutzung des ESPA-X Protokolls zur Anschaltung an den tetronik DAKS um bei Telefonalarmierung des Haustechnikers auch Informationen zur Störmeldung mitzugeben

Fazit des Projektes

- Neben den hohen Kostenvorteilen gegenüber einem „klassischen“ Gebäudeleitsystem konnte mit dieser Lösung auch eine vollständige Integration der Haustechnik in die Verwaltungssoftware und das IT-Monitoring der Akademie ohne große weitere Aufwände erreicht werden.

- Die klassische Trennung dieser beiden IT-Welten, Haustechnik und Office-IT, wurde damit erfolgreich aufgehoben.

Eine Umgebung für alle Störungen im Haus

Unsere Projekt Partner

- Durch ein starkes Team das Projekt erfolgreich in Zeit und Budget abgeschlossen

  - Holsten Systems GmbH, Thomas Holsten, Konzeption und Entwicklung Automatisierungssoftware für WAGO-Controller

  - Elektro Bauer, Elektroarbeiten

  - Buchner, Telko, LAN-Verkabelung

F & A

Fragen

Oracle APEX
In der Gebäudeleittechnik

Quellen

- EasyModbus
- PRTG
- WAGO PFC Controller
- Unify OpenScape Alarm Response (tetronik DAKS-Pro)
- Modbus
- ModbusTCP Testtool: www.modbustools.com
- SPS
- VPS (https://de.wikipedia.org/wiki/Verbindungsprogrammierte_Steuerung)

Quellen

- Oracle Dokumentation und Support Portal
- https://www.pipperr.de/dokuwiki/doku.php?id=prog:windows_dot_net_integration_plsql

- Wieder mal eine andere Script Library
  - https://github.com/gpipperr/OraPowerShell

- Bildmaterial : https://pixabay.com