WORKSHOP ON THE PREVENTION OF WATER POLLUTION DUE TO PIPELINE ACCIDENTS

International standards and recommended practices for the safety and environmental integrity level of international oil pipeline systems

Mr. Lars Bangert, Head of Unit "Pipeline Systems",
ILF Consulting Engineers, Germany

Thursday, 9 June 2005

AGENDA

1. Overview and Terminology

2. Functional Design Criteria for the SCADA System
   - Process requirements
   - Pipeline integrity requirements
   - Operational requirements

3. Functional Design Criteria for the Telecom System
   - Process requirements
   - Operational requirements
   - Pipeline integrity requirements

AGENDA

4. Pipeline Integrity
   - Design and Review of Safety Integrity Level
   - SCADA built in (internal) control mechanism
   - operational (external) control mechanism

5. SCADA Design Implementation

6. Telecom Design Implementation

1. Overview and Terminology

a) Automation & Control Terminology

- SCADA Supervisory Control and Data Acquisition
- ICSS Integrated Control and Safety System
- DCS Distributed Control System
- PLC Programmable Logic Controller
- FSC Fail Safe Controller

b) Purpose of (Pipeline) SCADA systems

- Integration of field equipment (e.g. actuator, sensor or pump) and small scale (unit) automation systems to the control centre computer system
- Transparent view for an operator on a complex process environment
- Efficient management/control of a remote process
- Support of pipeline integrity (for safety, environmental and commercial aspects)

1. Overview and Terminology

c) Purpose of (Pipeline) Telecom Systems

- data channels for the SCADA system
- voice channels for Operator instruction (control centre – local control room)
- Data channels for business WAN application
  (e.g. facility management, GIS-data warehouse, e-mail, etc.)

2. Functional Design Criteria for the SCADA System

a) Process requirements

- prevent critical process conditions
- Pump Station control
  (suction-/discharge-pressure control including overrides)
- (open) flow path monitoring
- slack line control

b) Pipeline Integrity requirements

- Integrated control and safety system (e.g. PSHH interlocks)
- SCADA built in monitoring mechanism (e.g. LDS, PCM)
- Programmed automatic ESD-Sequences
  (e.g. ESD-Pushbutton, Shut-Down due to Communication Failure)

2. Functional Design Criteria for the SCADA System

c) Operational requirements

- Remote Control via Control Centre
- Point-of-control (transfer procedures)
- simplified and summarized process information for the Operator
- Process Visualisation and Reporting (Process Displays and Alarm Handling)
- Integration of third party equipment
- Executive Control Sequences to support operator action

3. Functional Design Criteria for the Telecom System

Umwelt Bundes Amt
Für Mensch und Umwelt
UNECE

a) Process requirements

- redundant communication channels for SCADA system

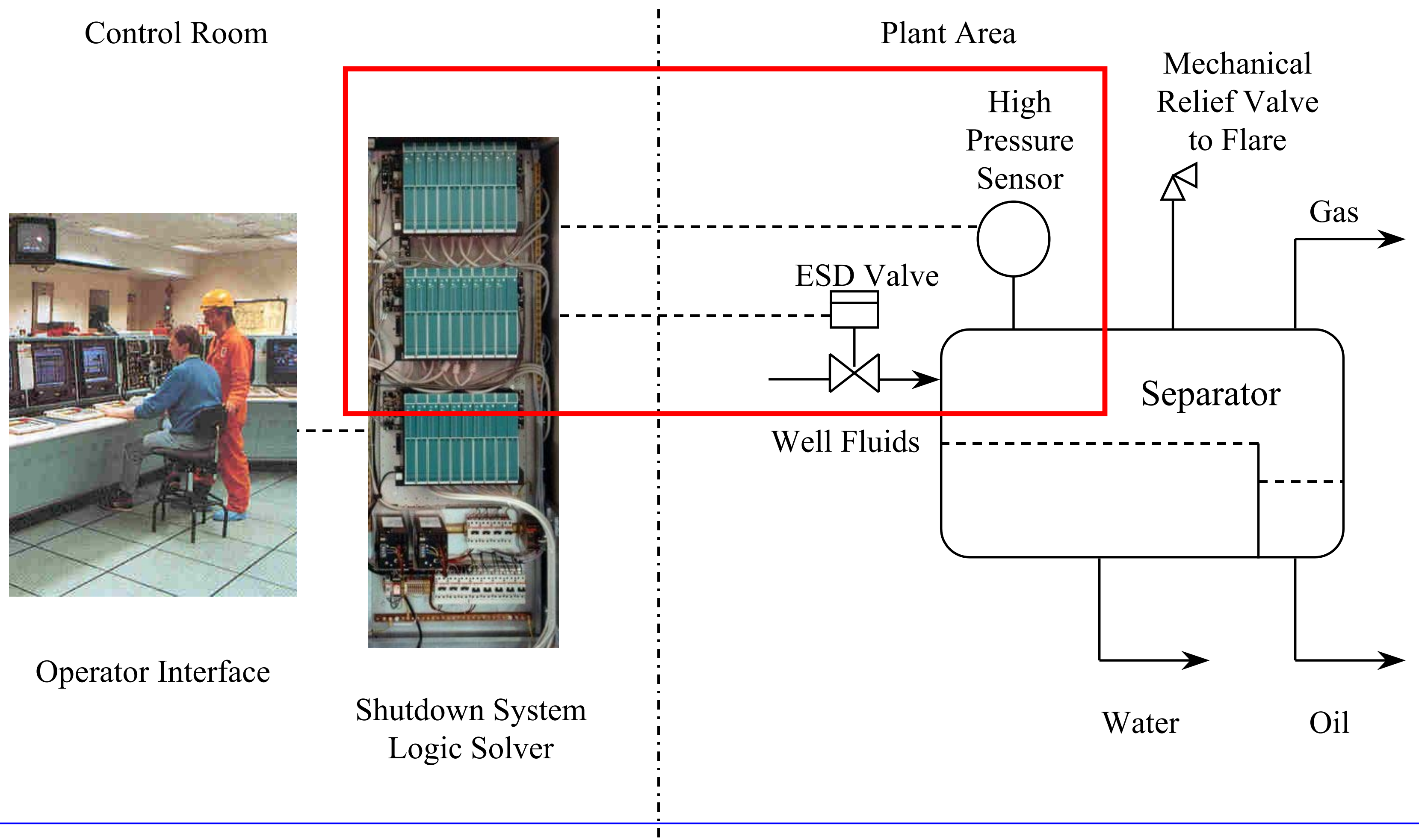
b) Operational requirements

- high system availability (➔ “no comms, no operation”)
- Voice channels for operator communication
- Data channels for business applications
- Video conference facilities

c) Pipeline Integrity requirements

- Reliable communication necessary for critical process data exchange (➔ Back-up communication link via satellite)
- Hotline functionality between operator control rooms

Example for a safety instrumented function



Various Reasons for SIL Assessment:

1. How much reliance do we need to place on the protective system to address the process safety concerns for a given application?
   or
   What integrity does it need to have?
   What is its required performance standard?

2. Engineer and maintain the system to
   - achieve the required integrity or
   - performance standard during its life

4. Pipeline Integrity-Design and Review of Safety Integrity Level (SIL)

3. national regulatory authorities expect it from us as prudent operators

4. Allows us to focus testing effort on the minority of safety systems which are critical for managing safety, environmental or commercial risks and spend less effort on the majority which are not critical

4. Pipeline Integrity-Design and Review of Safety Integrity Level (SIL)

Four Safety Integrity Levels are defined in IEC 61508 / IEC 61511

Safety Integrity Level (SIL)	Probability of Failure on Demand (PFD)	Probability of Success on Demand	Risk Reduction Factor (RRF)
4 (NR)	10^{-4} - 10^{-5}	99.99 - 99.999%	10,000 - 100,000
3	10^{-3} - 10^{-4}	99.9 - 99.99%	1,000 - 10,000
2	10^{-2} - 10^{-3}	99 - 99.9%	100 - 1,000
1	10^{-1} - 10^{-2}	90 - 99%	10 - 100

NR = Not Recommended

How to determine SIL?

- None of the standards recommend a particular qualitative or (semi-) quantitative method
- The standards suggest several methods in informative guidance as examples only
- No standard calibrates any of the suggested methods i.e. sets a tolerable risk level. This is up to the end user organizations.

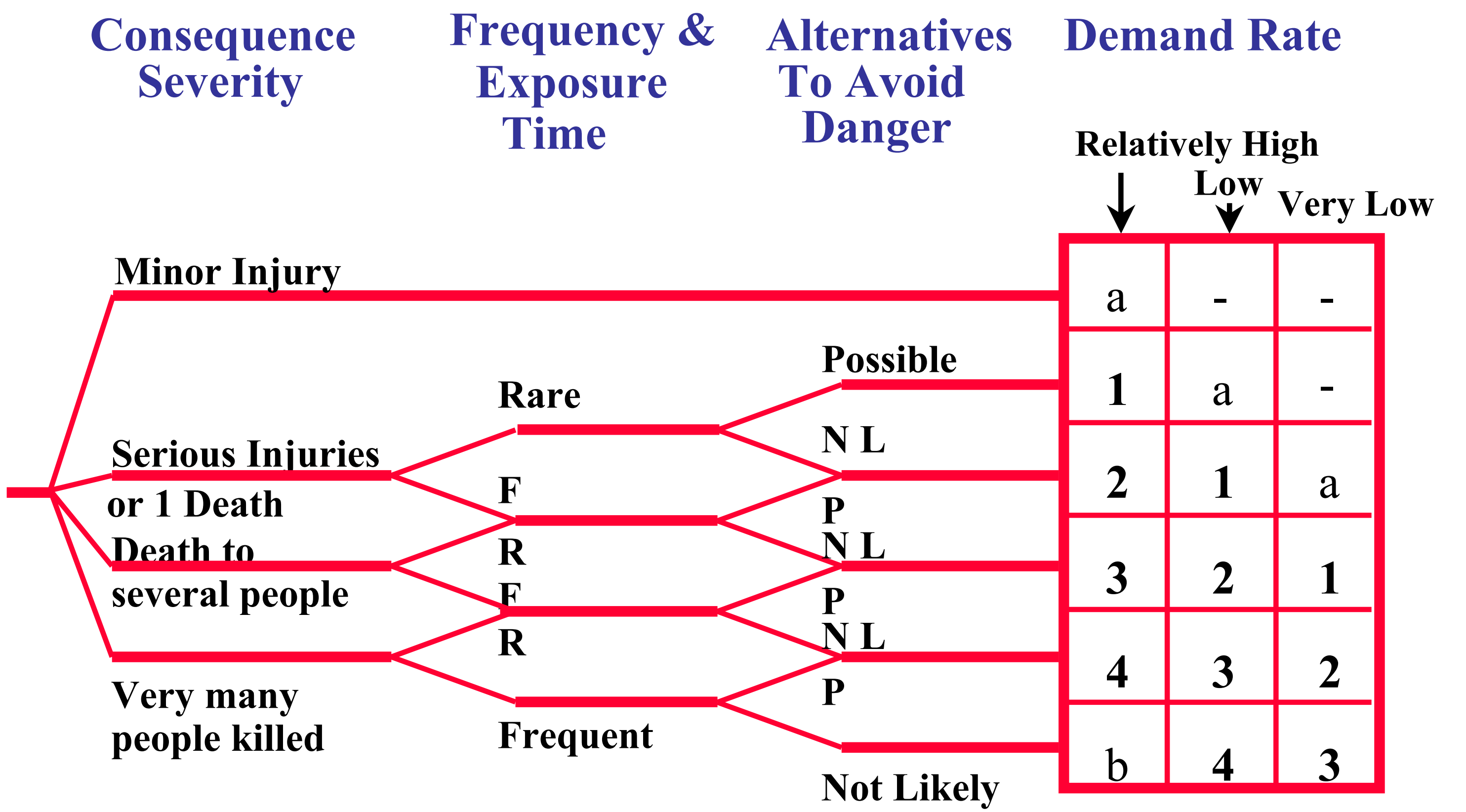
4. Pipeline Integrity-Design and Review of Safety Integrity Level (SIL)

Team approach, similar to Hazop

- Safety Engineer
- Process/Pipeline Engineer
- Operations Representative
- Instrument/Control Engineer
- Bring in other skills as required e.g. machinery

4. Pipeline Integrity-Design and Review of Safety Integrity Level (SIL)

Risk Graph from IEC 61508 / 61511

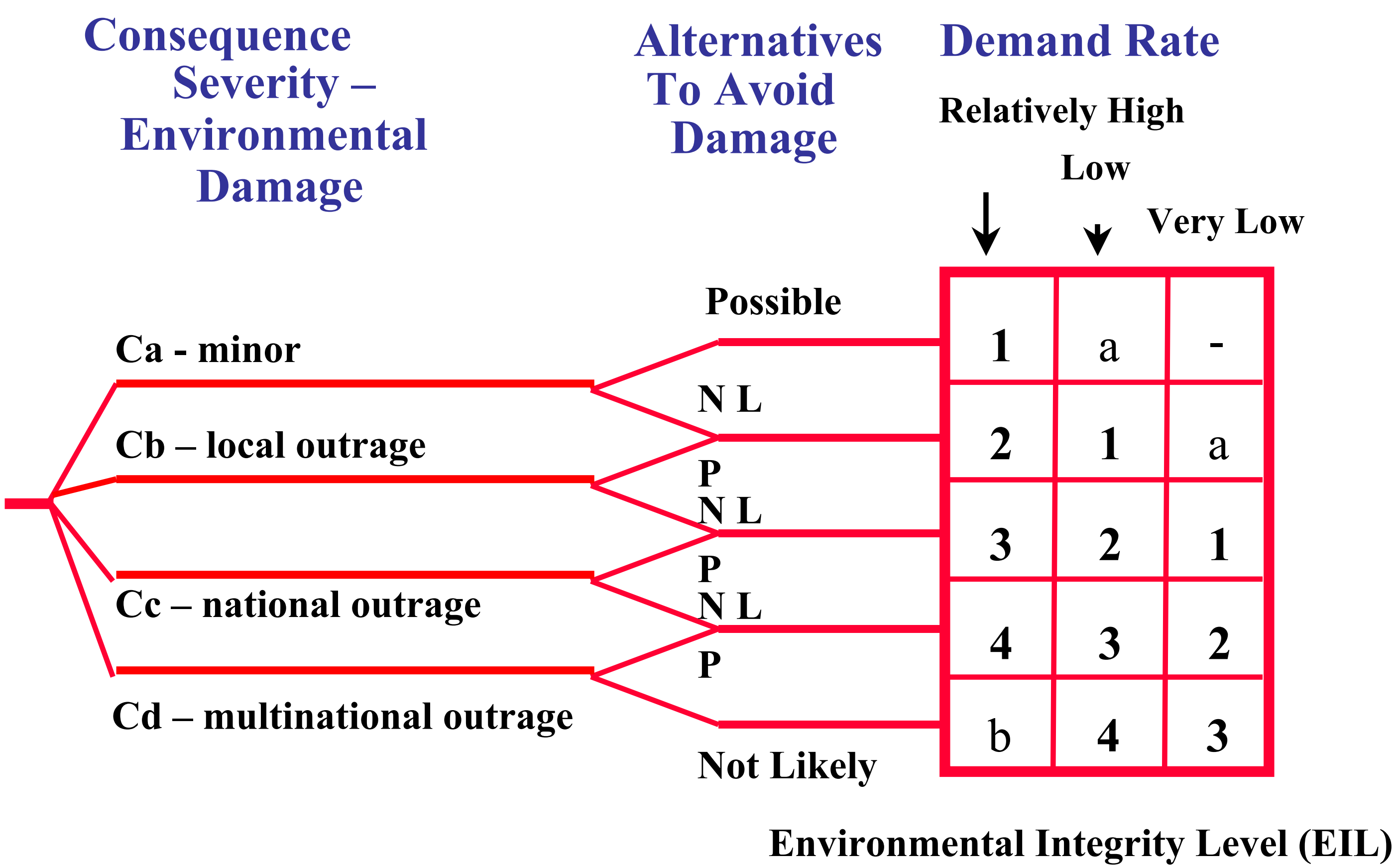


a = No special safety requirements
b = A single E/E/PES is not sufficient

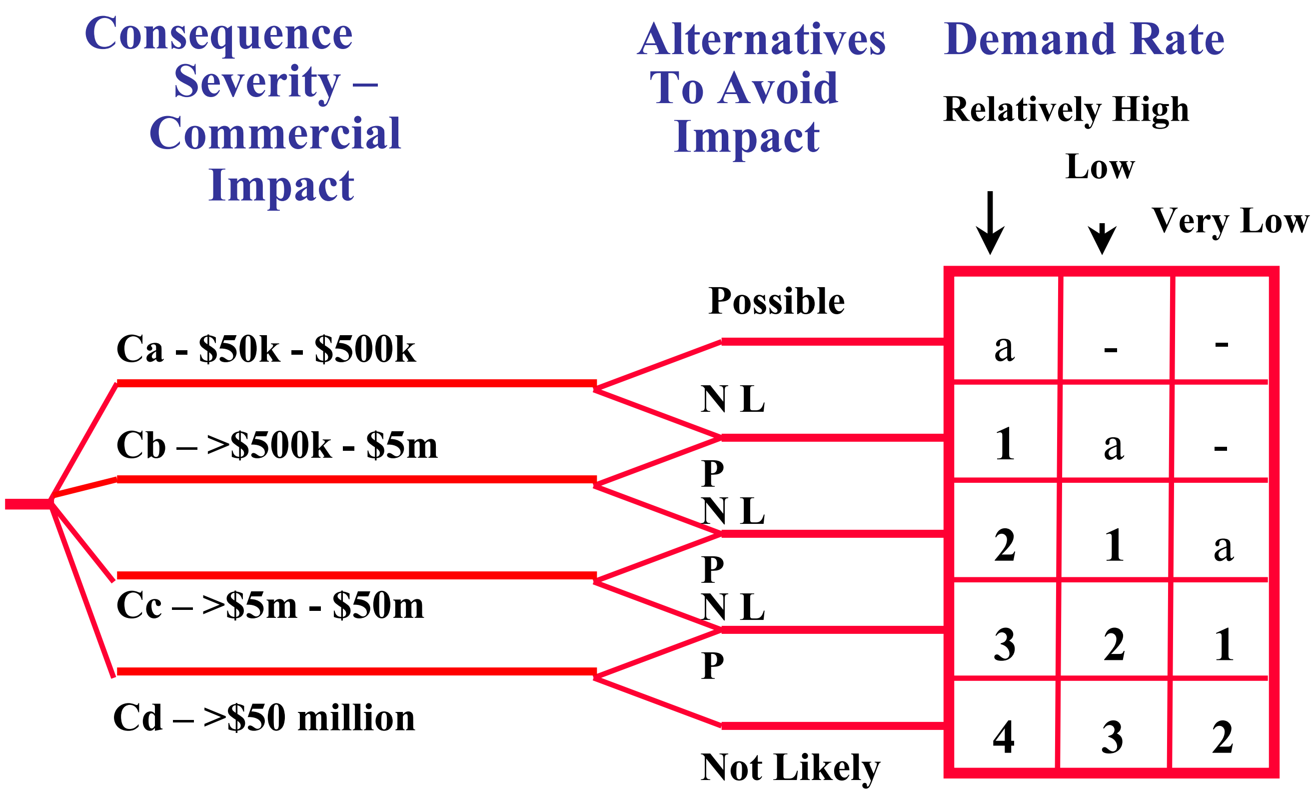
Safety Integrity Level (SIL)

4. Pipeline Integrity-Design and Review of Safety Integrity Level (SIL)

Environmental Risk Graph adapted from Safety Risk Graph



Commercial Risk Graph adapted from Safety Risk Graph



Commercial Integrity Level (CIL)

Calibrated to be risk neutral

Required Information for SIL determination

- P&IDs
- Design information on plant, PSV pressure ratings, pipeline hydraulic analysis, dynamic response to disturbances
- Cause and Effect Diagrams
- Setpoints of trips and margin from alarm levels

Umweltbundesamt

UNECE

Required Information for SIL determination

- Hazop reports
- QRAs – assumptions on event sizes and frequencies
- Personnel distribution and occupancy at the sites
- Proximity of the public to the sites
- Environmental impacts of loss of containment
- Value of partial and full pipeline shutdown per day

4. Pipeline Integrity-special SCADA applications to monitor Pipeline Integrity

a) Leak Detection System (LDS)

- Conventional Detection and Location Methods
  - Mass Balance
  - Pressure Drop
  - (negative) pressure wave
- Dynamic Model of the pipeline system

b) Pressure Cycle Monitoring System (PCM-System)

- Calculation of the remaining Pipeline system lifetime, based on monitored and classified pressure cycles

4. Pipeline Integrity-operational control mechanism

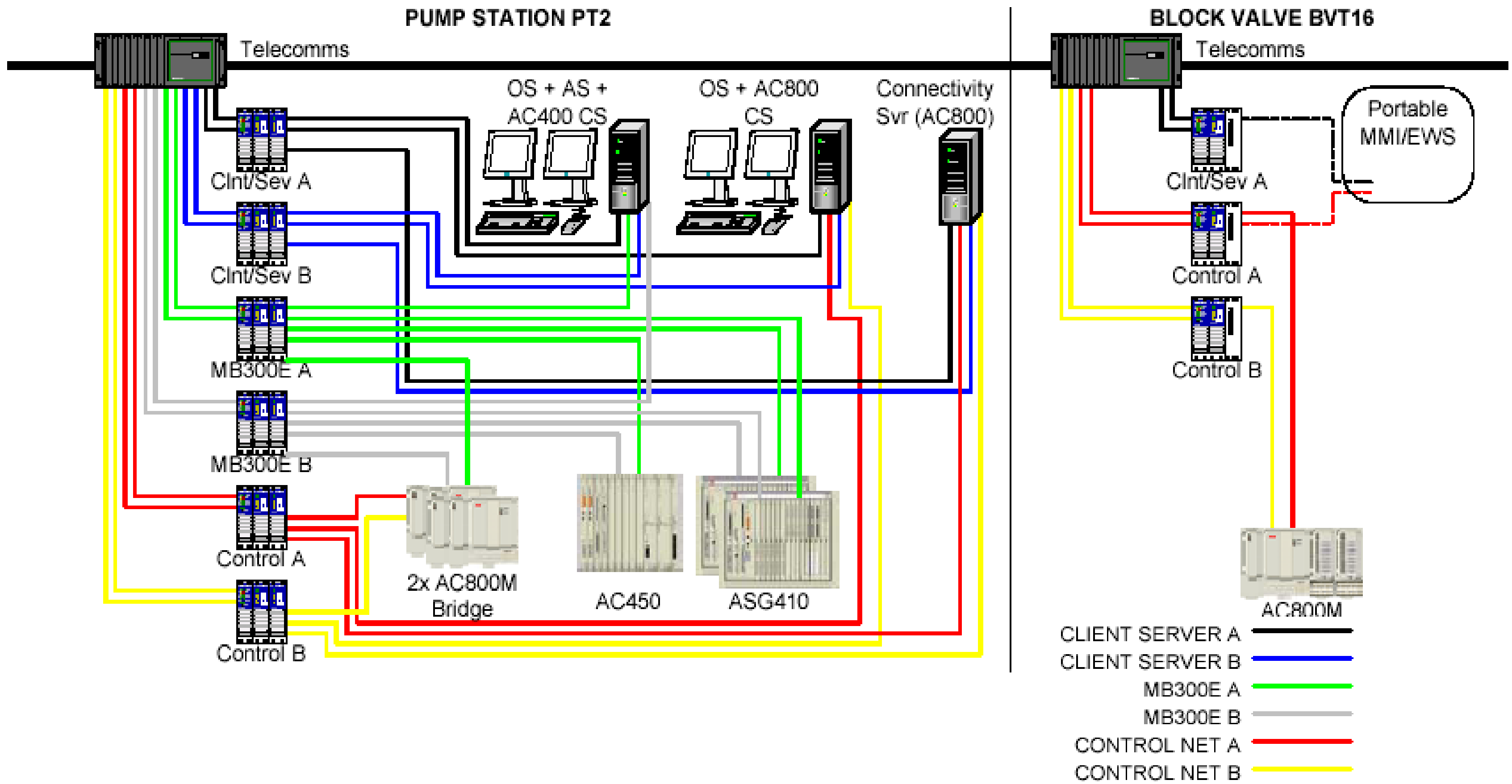
a) Intelligent pig runs

- Monitoring of internal pipe corrosion
- Detection of very small leakage

b) Flight surveys

- Monitoring of activities across the Pipeline Right-of-Way(e.g. construction work, erosion, any changes)

5. SCADA Design Implementation (Typical System Architecture)



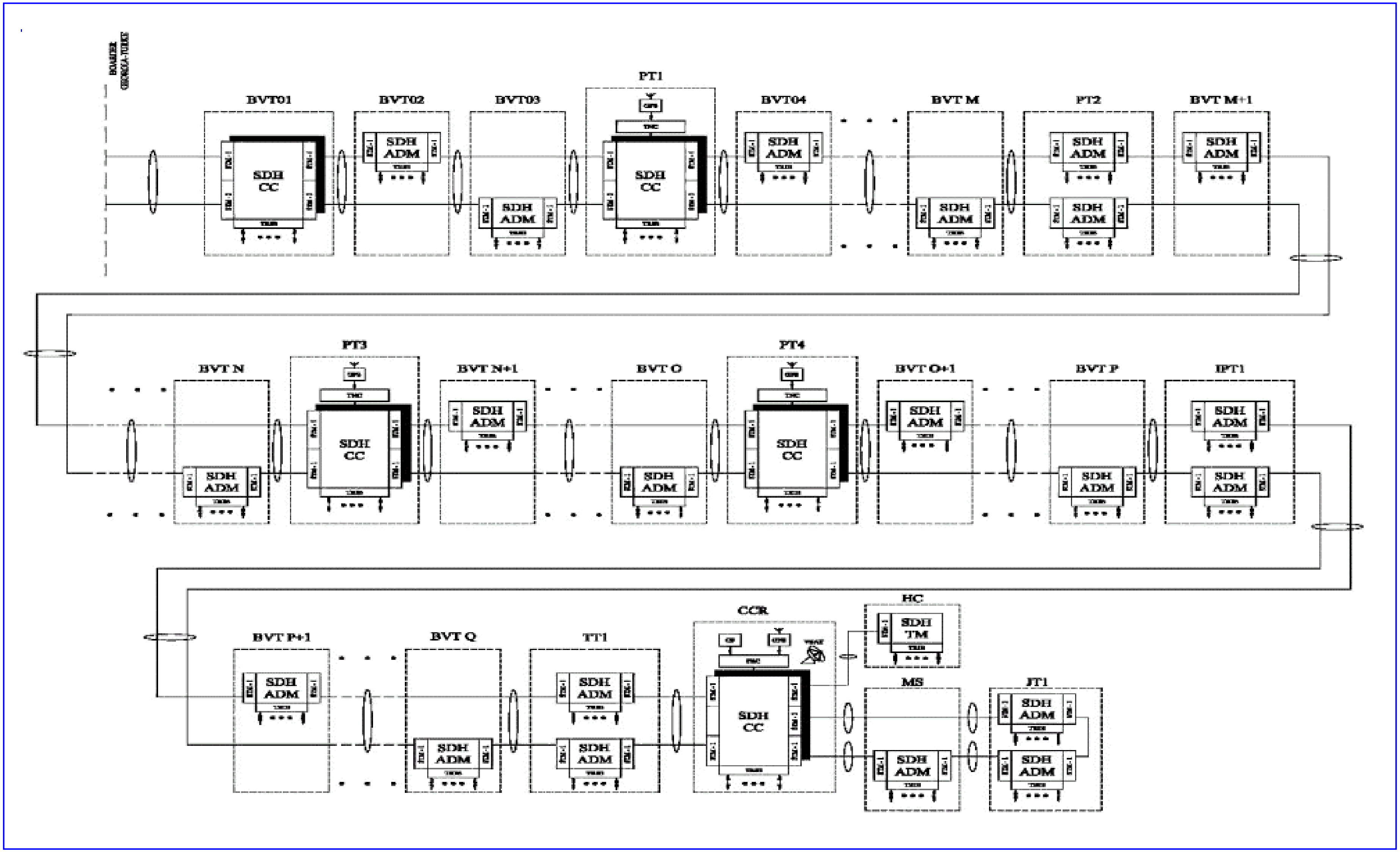
5. SCADA Design Implementation (Key Data)

	Az / Ge	Tr	total
Station PLC (ABB, AC450)	6	7	13
Station FSC (ABB, Safeguard)	10	8	18
BVS PLC (ABB, AC800M)	43	61	104
BVS FSC (ABB, AC31S)		52	52
HMI Operator Station (ABB, Operate IT)	7	15	22
Aspect Server (ABB, Operate IT)	5	6	11
Information Manager (ABB, Operate IT)	1	1	2
Network Manager (MS, Windows 2000)	1	1	2
Tank Farm Automation (ABB, TMAC)		2	2
LDS (Atmos Pipe & HAL)	2	2	4
Engineering Station	1	1	2

5. SCADA Design Implementation (Factory Acceptance Test)

6. Telecom Design Implementation (Transmission System Architecture)

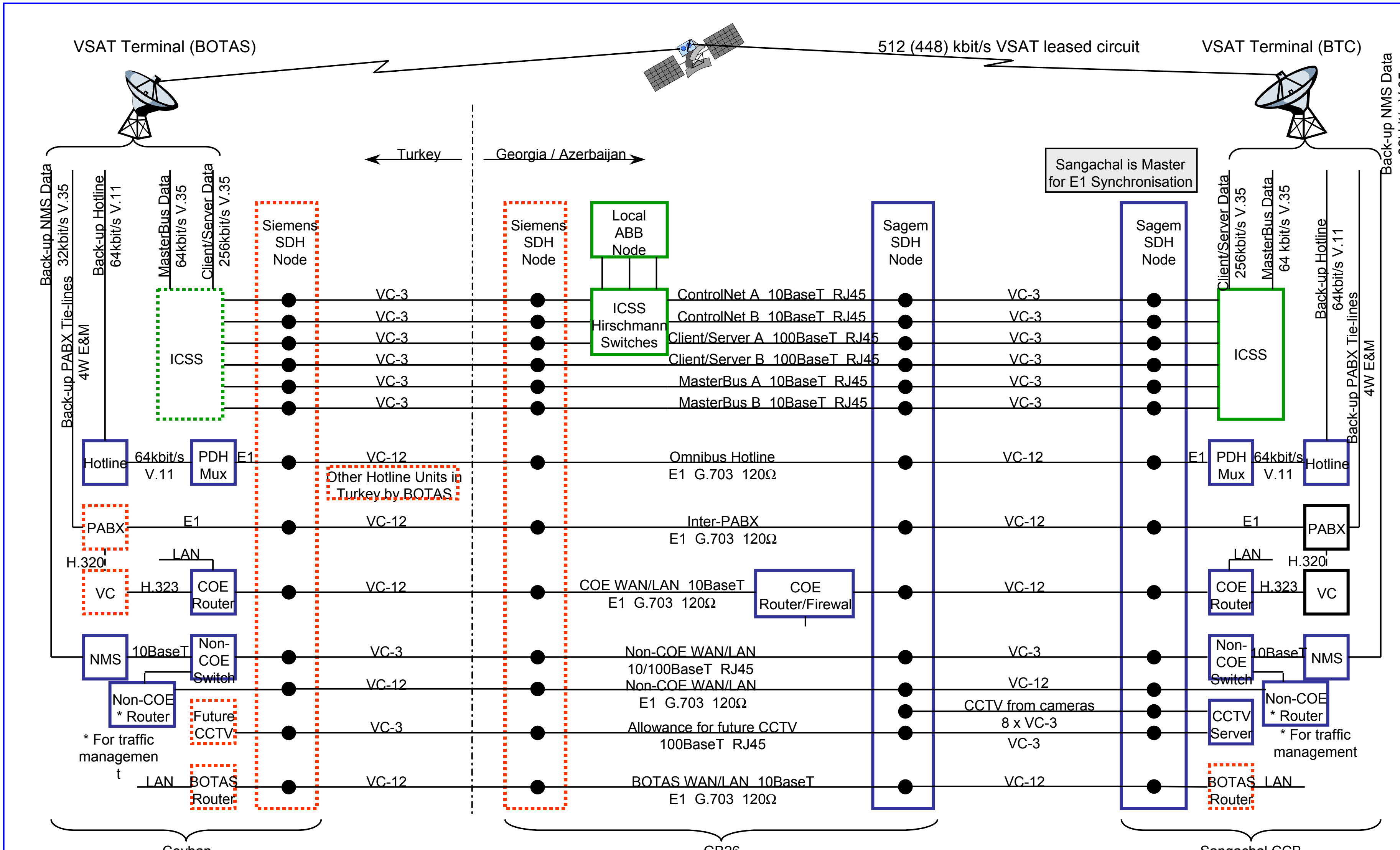
Umwelt Bundes Amt
Für Mensch und Umwelt
UNECE



6. Telecom Design Implementation (System Key Data)

- Medium: Fibre Optic Cable with G.652 fibres
- Transmission System: SDH STM-16 with
  - 1 SDH Terminal Multiplexes
  - 60 SDH Add/Drop Multiplexes
  - 5 red. SDH Cross-Connector
  - 1 Network Management System
- Backup System: VSAT (DAMA) system for the connection of the two control centres at Sangachal and Ceyhan in case of a primary telecom system failure
- Communication system: 14 PABX

6. Telecom Design Implementation (System Overview)



UNECE

iLF

Umwelt Bundes Amt
Für Mensch und Umwelt

Thank you for your attention

Lars.Bangert@muc.ilf.com