Survey of SCADA System Technology and Reliability in the Offshore Oil and Gas Industry

A Final Report to Dept. of the Interior, MMS TA&R Program
Program SOL 1435-01-99-RP-3995

by

Kelvin T. Erickson, Ann Miller and E. Keith Stanek,
Dept. of Electrical & Computer Engineering

Shari Dunn-Norman,
Dept. of Geological & Petroleum Engineering
University of Missouri-Rolla
Rolla, MO 65409

November 15, 2000

Abstract

This report concerns the use of commercial Supervisory, Control and Data Acquisition (SCADA) systems in the offshore oil and natural gas production industry. This report consists of three major parts:

- Current state of SCADA technology
- Reliability assessment of current SCADA technology
- Recommended MMS policy changes for operators that use SCADA systems

The major types of offshore facilities considered in this report are:

- Conventional and deepwater platforms
- Subsea systems
- Pipelines

The architecture and SCADA vendors are surveyed for these types of facilities. The reliability of platform, subsea, and pipeline SCADA systems is assessed. The effects of errors induced by humans and software is also considered.

Software development and quality assurance processes of several SCADA vendors were examined and a list of recommended best practices are included.

Table of Contents

Abstract i
Executive Summary 1
Survey of Current Offshore Systems which Employ SCADA 2
  Typical Offshore Systems which Employ SCADA 4
    Conventional and Deepwater Platforms 4
    Subsea Systems 5
    Pipelines 9
    Mobile Drilling Units 11
  Vendor Suitability for Offshore Systems 12
  Offshore SCADA System Features 14
    Hardware Features 15
    Communication Features 15
    Software Features 15
  Technology Trends 16
Reliability of Offshore SCADA Systems 17
  Fault Tree and Reliability Analysis 17
    Failure Probability for Hardware Components 22
    Development of the Surface/Subsea Fault Tree 22
    Calculating the Availability of the Top Event 35
    Non-Independent Basic Events 36
    Failure of the SCADA System 38
  Pipelines 40
  Human Error 41
  Software Reliability 42
  Operator Reliability Experience 43
  Summary of Reliability Analysis Results 44
  Software Quality 44
    Software Survey Results 45
Recommendations 47
References 48
Appendix A 51

List of Figures

1. Typical SCADA System Components 3
2. Distributed PLC Platform SCADA Systems 6
3. Centralized PLC Platform SCADA System 7
4. Deepwater Subsea SCADA System 9
5. Offshore Pipeline SCADA System 10
6. Mobile Drilling Unit SCADA System 11
7. Simple SCADA System 19
8. Fault Tree for Simple SCADA System 20
9. Reduced Fault for Simple SCADA System 21
10. Safety Flow Chart for Offshore Production Facility (from API RP 14C) 23
11. Fault Tree for Surface System 26
12. Subsea Control Subsystems 34
13. Fault Tree for Subsea SCADA 35
14. Fault Tree for Distributed Platform SCADA System 39
15. Pipeline Fault Tree 41
16. Human-induced SCADA Failure Fault Tree 42

List of Tables

1. Summary of Vendor Suitability for Each Type of Offshore Facility 13
2. Failure Data for Basic Events in Surface System Fault Tree 24
3. Failure Data for Basic Events in Subsea Fault Tree 40
4. Failure Data for Pipeline Fault Tree 40
5. Software-induced Failure Data for Basic Events in SCADA Fault Tree 43

Executive Summary

A comprehensive survey of SCADA systems in the oil and gas industry was prepared in order to assess the current state of SCADA technology and to focus the efforts of the reliability assessment. This survey included the three main categories of SCADA components: hardware, software, and communications. There are three major outcomes from this survey:

1. Generalized system architectures for each of the three major offshore oil and gas industry applications.
2. Summary chart of vendor suitability for each of the three applications.
3. Technology trends in offshore SCADA systems.

Using a generalized system architecture from the survey, the reliability of the system is estimated. The outcome of this reliability assessment is an estimate of

- Mean time between failures (MTBF)
- System availability
- Probability of facility damage or pollution release

The reliability was estimated using probabilistic risk assessment (PRA). A fault tree was constructed to show the effect of contributing events on system-level reliability. Probabilistic methods provide a unifying method to assess physical faults, contributing effects, human actions, and other events having a high degree of uncertainty. The probability of various end events, both acceptable and unacceptable, is calculated from the probabilities of the basic initiating failure events.

The probability of basic failure events (e.g., sensor failure, communication link failure) was determined mainly from OREDA (SINTEF, 1997). Some reliability data was obtained from current users.

Due to the minimal amount of software defect data and failure rates, the survey also includes a fact-finding study concerning software development process and software quality assurance (QA) procedures.

Based on the reliability assessment of current SCADA technology and interviews, guidelines for those operators that use SCADA systems are proposed. The specific recommendations include recommended software development and quality assurance best practices. Also, recommendations for further study are given.

Survey of Current Offshore Systems which Employ SCADA

According to ARC Advisory Group (1999), a system is classified as a supervisory control and data acquisition (SCADA) system when

> "…the system must monitor and control field devices using remote terminal units (RTUs) at geographically remote sites. The SCADA system typically includes the master stations, application software, remote terminal units and all associated communications equipment to interface the devices. The system must also include the controllers and I/O for the master stations and RTUs and also the system HMI and application software programs. It does not include field devices such as flow, temperature or pressure transmitters that may be wired to the RTU."

A generalized SCADA system for offshore oil and gas industry is shown in Figure 1. More specific system architectures are presented for four different types of facilities that employ SCADA systems offshore in waters under MMS jurisdiction. These facilities can be described as conventional and deepwater platforms, subsea systems, pipelines and mobile drilling vessels.

The information for the survey part of this report was gathered primarily from a representative set of offshore operators: BP-Amoco, Bridgeport Gas Distribution (Texaco), Chevron, Conoco, Exxon-Mobil, High Island Pipeline System, Marathon, Shell, Texaco, and Vastar. Dr Dunn-Norman and Dr. Erickson gathered information through drawings, meetings, and telephone conversations.

The next section of this report presents the system architectures for the four types of facilities that employ SCADA systems offshore. The SCADA architecture of mobile drilling vessels is presented, but excluded from further consideration since it is used strictly for monitoring and there is no remote control of actual drilling operations.

Next, the suitability of various SCADA hardware, software, and communication component vendors is assessed for platform, subsea, and pipeline facilities. In addition, the features of these components needed for an offshore facility are listed.

Technology trends in offshore SCADA systems are identified in the last part of this section.

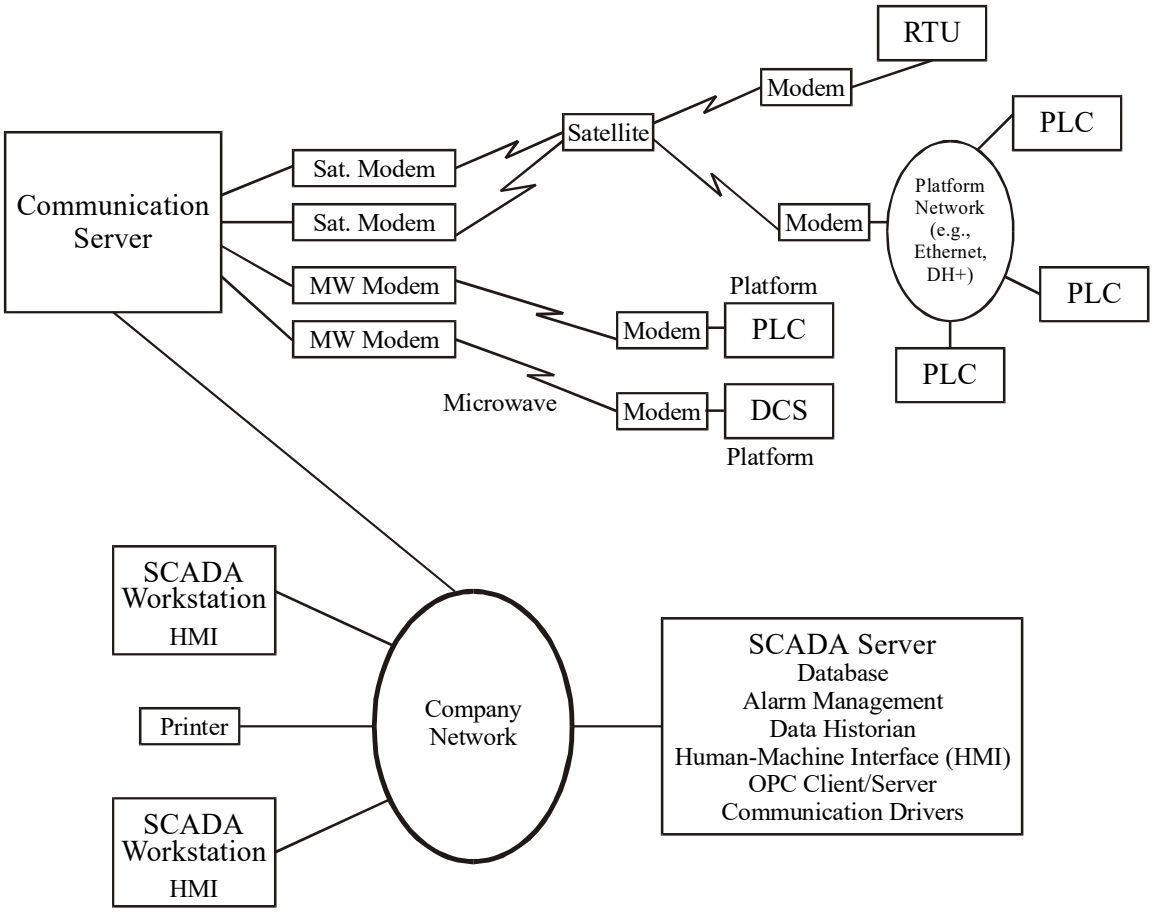

Figure 1. Typical SCADA System Components

Typical Offshore Systems which Employ SCADA

In the offshore oil and gas industry, SCADA systems are used in the following applications:

- Production monitoring and control
- Well monitoring and control
- Process monitoring and control
- Unmanned platform monitoring and control
- Pipeline systems
- Drilling

Each of these applications is addressed herein and provides an understanding of the range of functions the SCADA system performs.

This study identified four different types of facilities that employ SCADA systems offshore, in waters under MMS jurisdiction. These facilities can be described as conventional platforms, subsea systems, pipelines and mobile drilling vessels.

Conventional and Deepwater Platforms

A conventional platform is defined as a steel structure that consists of topsides and a jacket. The jacket is piled into the seabed and does not require any additional tethers or a mooring system for structural integrity. This type of structure has been used extensively to develop both oil and gas fields in the Gulf of Mexico (GOM) and offshore California. Conventional platforms may be small (tripods or four pile jackets) but many of these platforms are large (jackets with 8 piles or more), and include significant topsides and many wells.

Recent exploration successes in deepwater and technological advances have fueled trends toward deepwater developments. For deepwater, tension leg platforms or guyed towers are used with subsea production elements, such as subsea wells, templates, and manifolds. In these systems, the topside part of the structure is similar to that of conventional platforms. The subsea production elements are considered in the next section.

Wells drilled and completed from conventional or deepwater platforms are tied back directly to the platform, and the produced oil and gas flow directly from the production tubing into process facilities located on the platform.

Two major architectures of SCADA systems on offshore platforms have been identified:

- Distributed PLC
- Centralized PLC

The distributed PLC architecture is shown in Figure 2 and is typical of larger platforms. In this type of system, each major unit of the platform is controlled by a separate PLC. There is a platform communication network that connects the PLCs and the computers used for the Human-Machine Interface (HMI). The communication network is primarily used by the HMI/SCADA software to send commands to the PLCs and to receive information from the PLCs. There is generally limited information passing between the PLCs. Each major unit normally has a local operator panel to allow personnel to interact with that unit only. In this type of architecture, the safety system is generally handled by one of the PLCs. Typically, the platform communication network is redundant. If the primary network fails, communication is automatically switched to a redundant communication network. The platform is monitored from an onshore office by a microwave/radio/satellite link. The onshore office may perform some limited control functions, especially when the platform is evacuated due to bad weather.

Each PLC generally works autonomously from the other PLCs and will continue to control even if on-shore communication to the PLC is temporarily lost. However, if communication is lost for some significant time, the PLC will shut down the unit.

A deepwater platform has the same basic architecture as shown in Figure 2. The only difference is that the well SSV PLC and the equipment it controls is replaced by a subsea SCADA system, described in the next section.

The centralized PLC platform architecture is shown in Figure 3 and is more representative of smaller platforms and unmanned platforms. One PLC controls the platform equipment. In this case, the input/output (I/O) modules connected directly to the equipment communicate with the platform PLC over a specialized network, generally called a remote I/O network. Some larger units, e. g., a turbine generator may have a separate PLC, as in the distributed platform architecture. In this architecture, the safety system is generally only monitored by the PLC.

Subsea Systems

Subsea technology has evolved rapidly since the 1980s and many subsea wells now exist offshore in the GOM. The term *subsea systems* refers to clusters of subsea wells, or the combination of subsea wells tied to another host facility.

A subsea well is a well completed with the wellhead and tree on the seafloor. Oil and gas produced from each subsea well flows through an individual flowline (on the seafloor), to a production manifold (also located on the seafloor). The production is combined at the manifold and produced back to a host facility, normally through a flowline and riser.

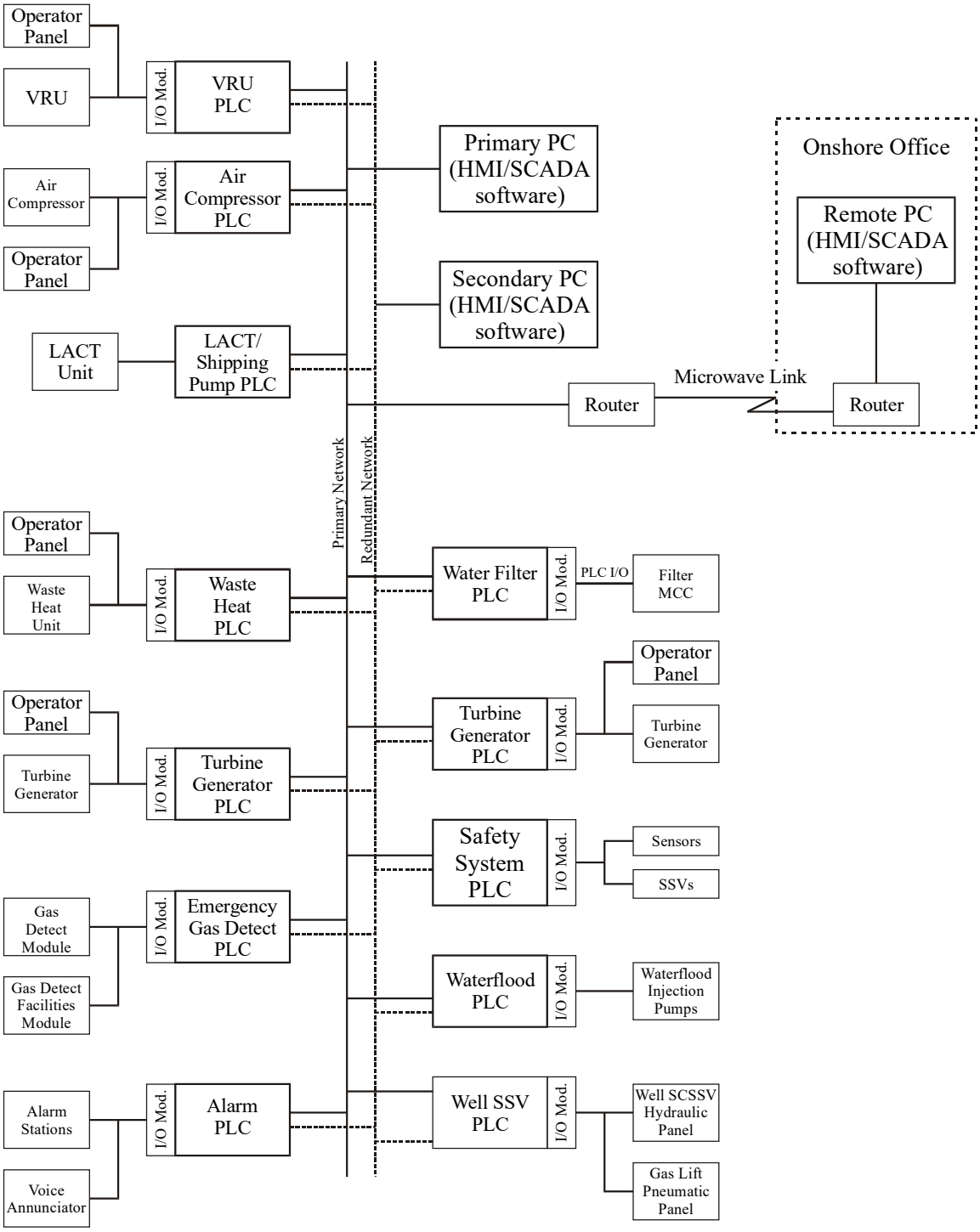

Figure 2. Distributed PLC Platform SCADA System

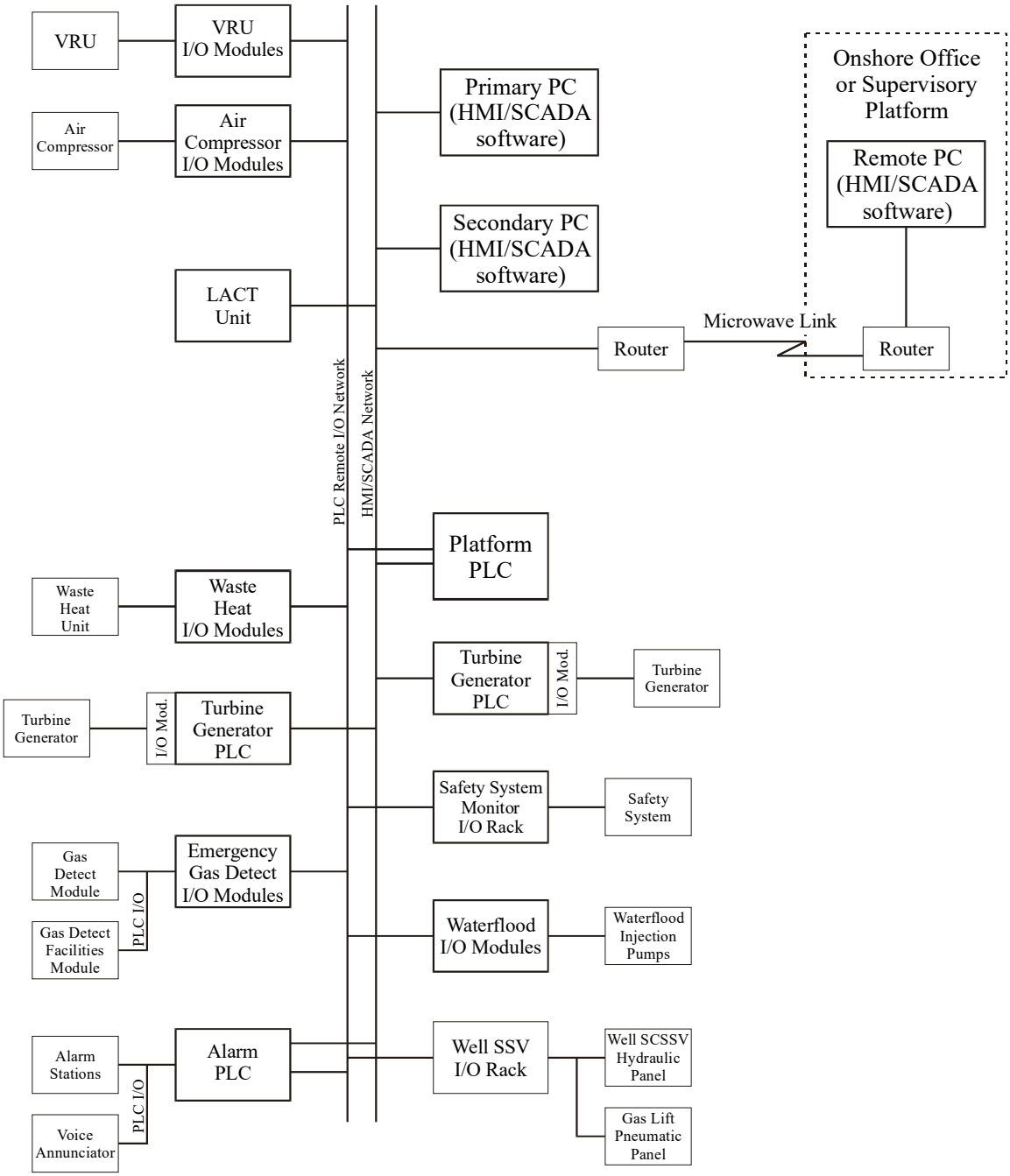

Figure 3. Centralized PLC Platform SCADA System

The host facility can be a conventional steel platform; a tension leg platform (TLP); a floating production, storage and offloading facility (FPSO), a caisson, spar or guyed tower. Regardless of the type of host facility, the host acts as the point where produced oil and gas is separated, treated, metered and sold.

In subsea systems, one operator may have developed a field many miles from the nearest host facility. Additionally, another company may operate the host facility. Sharing production facilities in this manner is common practice, as this reduces development costs for more marginal, outlying fields.

Currently in the Gulf of Mexico, there is significant emphasis on developing oil and gas reserves in deepwater (> 2000 ft) and this trend will fuel additional growth in the use of subsea facilities tied to a host facility.

Figure 4 depicts a typical arrangement between subsea wells producing to a host facility. The main control for a group of wells sharing a subsea manifold is generally connected to the host facility communication network. The control is handled by a redundant PLC on the host facility, which is connected to a redundant serial communication network to the subsea facilities. An electrical umbilical provides the communication to subsea facilities. Flying leads connect each subsea well to the manifold.

A multiplex electrohydraulic control system is used to perform the functions specified. No RTUs or PLCs are located subsea.

The multiplex electrohydraulic controls are piloted hydraulic controls with the pilot function replaced by an electrical signal. Individual tree and manifold control is provided by subsea control pods. These modules contain the valving and associated electronic/electric circuits required for routing the hydraulic fluid to the various valve and choke actuators. All monitoring of subsea system status is accomplished in the subsea modules. Individual well control pods also monitor pressure and temperature data, control subsurface safety valves, chemical injection valves and annulus valves. Most subsea systems include redundant control modules.

During workover operations, the workover vessel assumes control of the subsea well and provides the same valve control operations provided by the host facility. The vessel provides monitoring and shut-in control for the tree (if it is in place) or for the blowout preventer stack if the tree has been removed.

Older subsea control systems may include a subsea junction box on the template for distribution of electric power signals to the subsea control modules. None of the newer deepwater systems investigated in this study included subsea junction boxes.

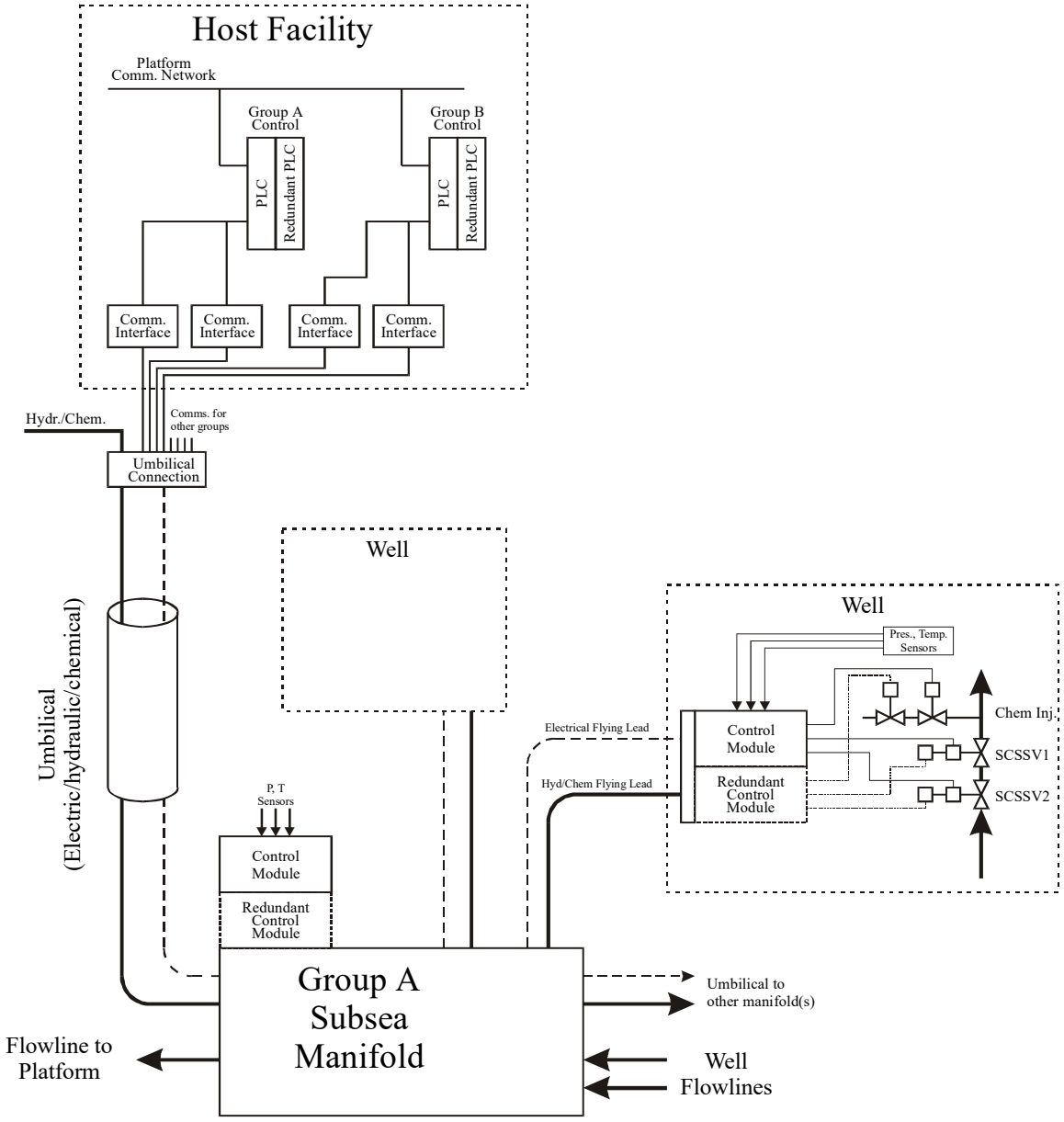

Figure 4. Deepwater Subsea SCADA System.

Pipelines

On the topsides of a conventional platform or any host facility, the oil and gas is separated, treated, metered and sold. In most cases, after metering, the oil and gas are transported to shore through a large diameter (24-36 inch) steel pipeline. These pipelines are operated single phase (oil only, gas only) to minimize pressure losses from multi-phase flow effects.

The company that operates the host facility does not necessarily own the pipeline that transports the oil and gas from a particular host facility. Most frequently, another company owns the pipeline or a network of pipelines from the platforms. For that reason, both parties meter the product so that produced volumes can be compared with those purchased and transported to shore. Inlet pressure and delivery pressures are recorded continuously and are compared to assist in determining leaks.

Most pipelines in the GOM are in less than 300'of water. No subsea booster pumps are included in the lines and the lines are serviced with conventional or saturation diving.

Figure 5 depicts a typical architecture of a pipeline SCADA system. The pipeline SCADA system is separate from the other platform systems, though it is attached to the platform. There is an RTU (which often is a PLC) that monitors the production from the platform as well as the total flow through the pipeline. The SCADA system may command a valve to close the flow from a platform, but this is generally used only for emergencies (e.g., upstream pipeline break). Communications with the onshore office is by a satellite or microwave communication network.

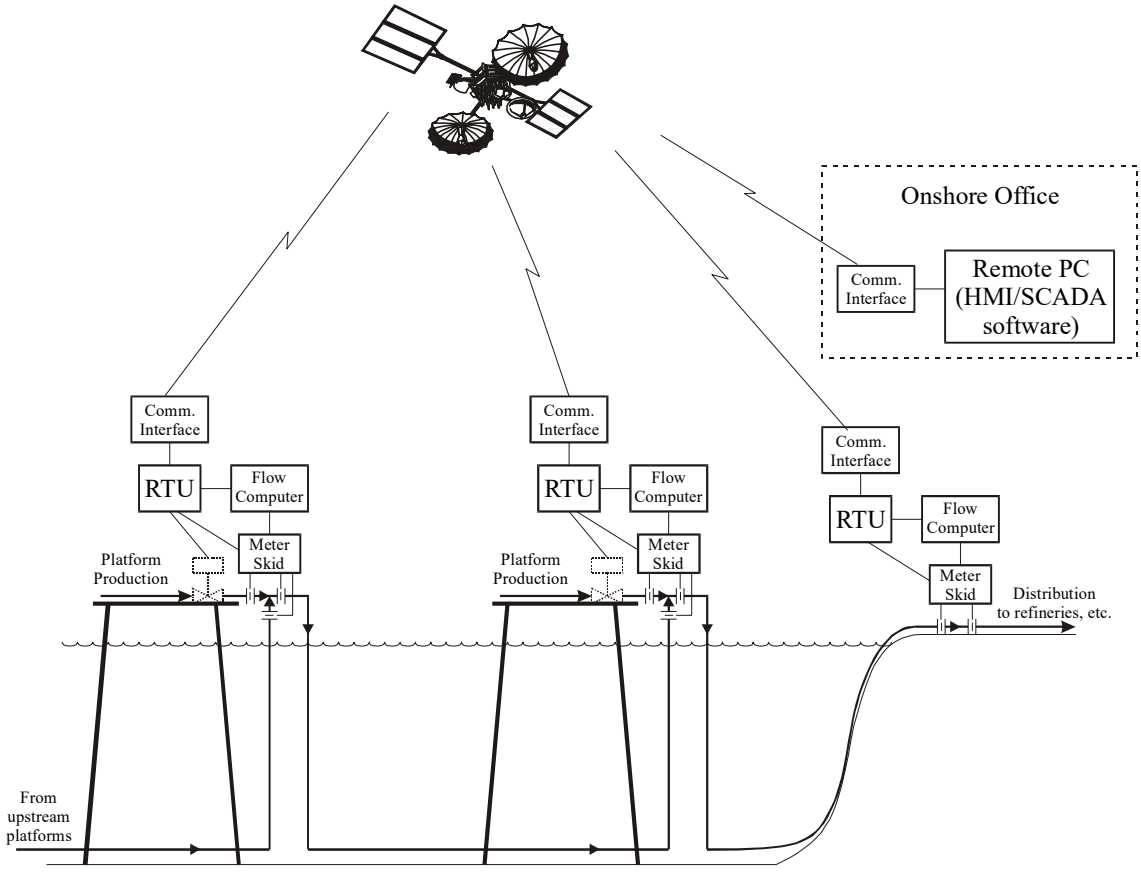

Figure 5. Offshore Pipeline SCADA System.

Mobile Drilling Units

Offshore drilling vessels include jackup rigs, semi-submersibles and drillships. Jackups rest on the seafloor and are restricted, for the most part, to waters less than 400 ft. Semi-submersibles and drillships are floating rigs, and they are the main units for drilling in deeper waters.

The floating drilling units must maintain their position over the drilling location. Typically the units use a combination of dynamic positioning and spread mooring. In deepwater, only dynamic positioning is used.

Dynamic positioning requires a constant monitoring of sea and wind conditions to coordinate and control the thrusters used to keep the drilling vessel on location. Dynamic positioning is a critical function necessary to keep the vessel on station.

During the drilling operation, measurement while drilling (MWD) data, mud logging data, drill steam test data and mud properties are measured at regular intervals.

In this study, it was determined that SCADA systems are only being used on the most advanced mobile drilling vessels and that these systems are used to report drilling data back to an onshore office location, as shown in Figure 6. No drilling vessels allowed or provided for remote control of actual drilling operations or positioning of the rig.

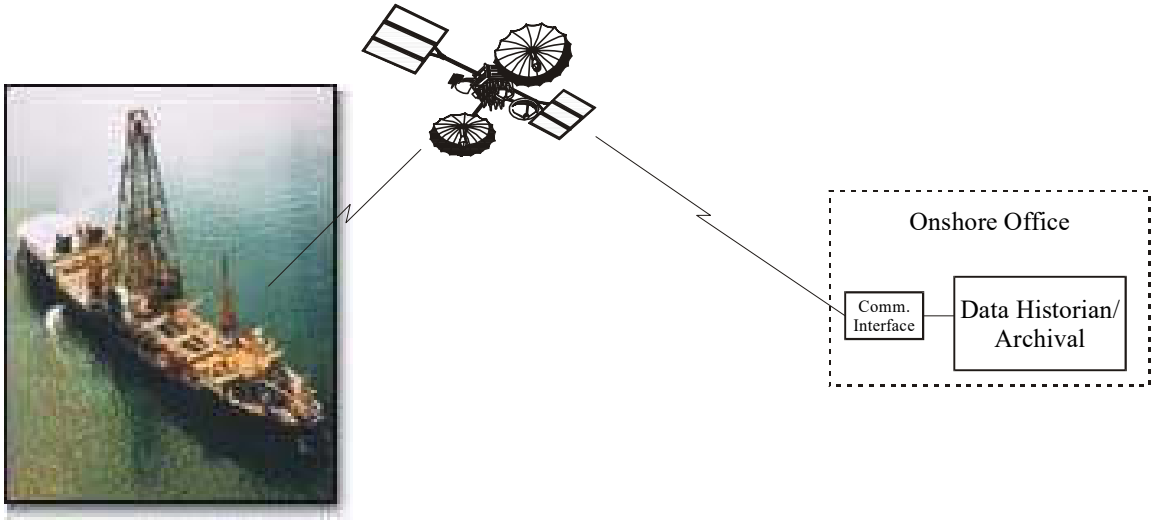

Figure 6. Mobile Drilling Unit SCADA System.

Vendor Suitability for Offshore Systems

In this section, the vendors of components used in offshore oil and gas SCADA systems are listed, along with the type of component used in the three applications. The types of products are listed for each vendor, and then the product features that are needed in offshore applications are listed.

The three main categories of components that comprise a SCADA system are hardware, software, and communications. Among the vendors, no one seems to support both short-distance (local-area networks) and long-distance (e.g., satellite, microwave) communications. Therefore, communication components are divided into two categories, leading to the following four categories of SCADA system components:

- Hardware – programmable logic controllers (PLCs), remote terminal units (RTUs), and distributed control systems (DCSs).
- Software – SCADA software package consisting of the database, human-machine interface (HMI), alarm management, and data historian; communication drivers; object linking and embedding for process control (OPC) modules; and the operating system.
- Short-distance communication networks – local-area networks, (e.g., Ethernet, Modbus), remote I/O networks, and control networks at the remote units.
- Long-distance communication networks – satellite, microwave, telephone, and radio communication; including modems if distinct from other hardware components (e.g., PLC).

Vendors for the computers that execute the software are numerous and so are not considered in this report.

According to existing SCADA system surveys (ARC Advisory Group, 1999; ISA, 1998), there are currently about 30 vendors of SCADA hardware and software and another 10 vendors of just SCADA software. These lists were narrowed to only include vendors involved in offshore oil and gas operations. In addition, after visiting offshore operators, some vendors were added to the list. Information was acquired from the following operators: BP-Amoco, Bridgeport, Chevron, Exxon-Mobil, High Island Pipeline, Marathon, Shell, Texaco, and Vastar.

Vendor suitability for each of the three types of facilities is summarized in Table 1. For each vendor, the types of components supported for each of the three types of facilities is shown by a letter as follows:

H – hardware
S – software
L – local-area network
D – distant network (e.g., satellite, microwave)

For example, a vendor that only supplies RTU hardware is shown as “H”, where a vendor that sells hardware, software, and local-area networks is shown as “HSL”. In addition,

some vendors marked with (*) have products suitable in offshore oil and gas SCADA systems, but were not indicated by the surveyed operators.

Table 1. Summary of Vendor Suitability for Each Type of Offshore Facility

Vendor	*Platform*	*Subsea*	*Pipeline*
AT&T Clearlink	D		D
Bailey	H		
Chevron WinSCADA	S		
Cisco	D		
CI Technologies (*)	S		S
Daniel Industries	H		H
Datacom	D		D
Data-Linc Group	D		
Elliott	H		H
Flow Automation	H		H
GE/Fanuc	HLS		HS
Halliburton	H		
Hewlett-Packard			S
Iconics (*)	S		S
Intellution (*)	S		S
Kongsberg Offshore a.s.		HL	
Moore Products	HS		
New Bridge	D		D
Oilfield Systems, Inc.	S		S
RealFlex Systems	S		
Rockwell Automation	HSL	HL	H
Schneider Automation (Modicon, Square D)	HL		H
Shell/BP/Amoco	D		D
Siemens	HL		
Stratacom	D		D
Teledyne Brown (*)	H		H
Texaco RTU			H
Tokheim Corp.	H		H
VSAT	D		D
Wonderware	S	S	S

The products and services from each of the vendors listed in Table 1 are:

AT&T Clearlink – satellite dish transponder
Bailey– Net 90 distributed control system
Chevron WinSCADA – In-house SCADA software
Cisco – Communication network routers, long-distance network switch

CI Technologies – Citect HMI package, drivers for many PLC and RTU vendors
Daniel Industries – remote terminal unit
Datacom – digital microwave network provider; loop topology provides 2 paths to onshore
Data-Linc Group – Ethernet radio modems
Elliott – remote terminal unit
Flow Automation – remote terminal unit
GE/Fanuc – H: Series 90-30 and 90-70 PLCs; the 90-30 often used in place of traditional RTUs; L: Ethernet, Series Ninety Protocol (SNP); S – Cimplicity HMI package
Halliburton – GFC-332 flow computer (RTU)
Hewlett-Packard – RTAP HMI software
Iconics – Genesis32 HMI package, drivers for many PLC and RTU vendors
Intellution – Fix Dynamics HMI package, drivers for many PLC and RTU vendors
Kongsberg Offshore a.s – subsea control equipment packages
Moore Products – APACS distributed control system
New Bridge – digital multiplexer to microwave
Oilfield Systems Inc. – Plant Information (PI) data archival software
RealFlex Systems – SCADA software
Rockwell Automation – H: PLC-5 and SLC-500 PLCs; the SLC-500 often used in place of traditional RTUs; L: Ethernet, ControlNet, Data Highway+, Remote I/O; S: RSView HMI package, drivers for non-RA equipment, though not as many as Wonderware
Schneider Automation – H: Modicon and Square D PLCs, often used in place of traditional RTUs; L: Modbus, Modbus+, Sy/Max networks
Shell/BP/Amoco – digital microwave network
Siemens – H: 505-series (ex-Texas Instruments) PLCs; L: Ethernet, TIWAY, Profibus-DP
Stratacom – long-distance network switch
Teledyne Brown – remote terminal unit
Texaco RTU – In-house RTU
Tokheim Corp. – remote terminal unit
VSAT – satellite communications provider
Wonderware – InTouch HMI package, drivers for most PLC and RTU vendors, special drivers are often developed by users and third parties

Offshore SCADA System Features

The hardware, software, and communication features needed for offshore facilities were determined from prior knowledge and refined based on information from the surveyed operators. Note that the lists are representative and many operators do not consider all of the features in any given list. In addition, most companies standardize the hardware/software/communication vendor selection. The most common choices are:

Hardware – Rockwell Automation (Allen-Bradley) PLC-5 and SLC-500
Software – Wonderware InTouch
Communication – DataCom or Shell/BP/Amoco digital microwave system

Hardware Features

According to the surveyed operators, hardware products are selected for offshore platform and pipeline systems based on many of the following features:

- Proven reliability
- Ease of maintenance
- Ease of modification
- Discrete and analog I/O
- Ruggedized
- Division 2 environment
- Intrinsically safe
- Redundancy (though a minority of operators use this feature)

The desired features of subsea systems are considered separately since the environment for these systems is very different from platform and pipeline systems:

- Proven reliability
- Ruggedized
- Redundancy

Communication Features

According to the surveyed operators, communication products are selected for offshore systems based on the following features:

- Redundancy
- Ease of modification
- Supported protocols (most popular: Ethernet, Data Highway+)

Software Features

According to the surveyed operators, software products are selected for offshore platform and pipeline systems based on many of the following features:

- Operating system supported (Windows NT or UNIX)
- Range of supported PLC/DCS/RTU vendors and communication protocols
- Ease of modification
- Intranet Web (firewall to outside of company)
- Alarming
- Historical trending
- Built-in diagnostics
- Reliability

Many of the offshore operators seem to use Wonderware InTouch because it is easy to learn and modify and it supports a large number of PLC and RTU vendors. In addition, users and third parties often develop interfaces for special or obscure equipment.

Technology Trends

As a result of gathering the information for this report from offshore operators, the following technology trends in SCADA systems for offshore oil and gas facilities were identified:

- **Replacement of pneumatic safety systems with electronic safety systems.** According to the operators that have been using electronic safety systems, electronic systems are much more reliable and require less maintenance.

- **Remote terminal units (RTUs) replaced by programmable logic controllers (PLCs).** The PLC hardware and software is easier to modify.

- **Remote operation of platforms.** One operator (Chevron) operates many of the platforms from onshore. Another operator (Texaco) only operates the platforms from onshore when the platforms have been evacuated due to storm conditions. Many operators are reluctant to operate platforms from onshore, but with increasing demands to cut costs, removing personnel and remotely operating platforms is one means to that end. Preliminary guidelines for remote startups and remote operations are currently being formulated as a result of this trend.

- **Use of Windows NT operating system.** This seems to be nearly universal.

- **Use of commercial off-the-shelf (COTS) hardware/software.** Most operators do not have the resources to support in-house product development. Most of them are phasing out the systems developed in-house.

- **Use of integrated software architectures.** One of the best practices cited in the software reliability (below) is the development of a common software framework that will support multiple software components in a seamless manner.

Reliability of Offshore SCADA Systems

The reliability of the complete SCADA system (hardware, software, and communication network) was estimated. The outcome of this reliability assessment provides

- Mean time between failures (MTBF)
- System availability
- Probability of facility damage or pollution release

The above was estimated for the platform, subsea, and pipeline systems.

As the study progressed, we found that vendors would not divulge reliability information about their products. Therefore, reliability information from SINTEF (1997) was used to assess the reliability of the offshore systems. Since SINTEF (1997) does not cover software or human-induced failures, other data sources were used to estimate the reliability for these failures. Redundancy for subsea systems was considered.

The types of failures included:

- Hardware failures
- Software failures
- Human-induced failures
- Communication link failures
- Fire/explosion

Fault Tree and Reliability Analysis

The reliability assessment of current SCADA technology has two major directions:

1. Calculation of a reliability index for the SCADA system as a whole, including sensors, modems, communications channels, servers and the SCADA workstation. The form of this index is the system unavailability.

2. Calculation of the probability of a top event during a given year. This top event is facility damage or a significant oil spill.

The calculations are relatively simple if the system is a series system in a reliability sense. This is true of many electronic or mechanical systems. Once the reliability performance of each component in the chain is found, the overall system performance is easily calculated. For instance, if the availability of each component of the system can be found, the overall system availability is just the product of the component availabilities. Similar, relatively simple calculations can be done to find the probability of system

failure, or the mean time between system failures. For instance, if $\lambda_i, i = 1, n$ are the n component failure rates, then the system failure rate is

$$\lambda_{system} = \sum_{i=1}^{n} \lambda_i$$

The system reliability, assuming constant failure rates and no repair, is

$$R(t) = e^{-\lambda_{system} t}$$

The system mean-time-to-failure is

$$MTTF_{system} = \frac{1}{\lambda_{system}}$$

The component availabilities can be found if the constant repair rates for the n components are known to be $\mu_i, i = 1, n$. In that case the availability of the i^{th} component is

$$A_i = \frac{\mu_i}{\lambda_i + \mu_i} = \frac{MTTF}{MTTF + MTTR}$$

and the system availability is

$$A_{system} = \prod_{i=1}^{n} A_i$$

The latter calculation is more challenging but it contains the most pertinent information.

Most systems, however, are not simple series systems and therefore more powerful techniques such as fault tree analysis must be used.

Probabilistic risk assessment (PRA) was used to assess the effect of contributing events on system-level reliability tree (Billinton and Allan, 1992; Henley and Kumamoto, 1992). Probabilistic methods provide a unifying method to assess physical faults, contributing effects, human actions, and other events having a high degree of uncertainty. The PRA was performed using fault tree analysis. The probability of various end events, both acceptable and unacceptable, is calculated from the probabilities of the basic initiating failure events.

The fault tree model serves several important purposes. First, the fault tree provides a logical framework for the failure analysis and precisely documents which failure scenarios have been considered and those that have not. Second, the fault tree is based on well-defined Boolean algebra and probability theory. The fault tree shows how events combine to cause the end (or top) event, and at the same time defines how the probability of the end event is calculated as a function of the probabilities of the basic events. Thus,

the fault tree model can be easily changed to accommodate systems consisting of components from one vendor as well as components from mixed vendors (e.g., software vendors and hardware vendors). The fault tree analysis also illuminates the "weak points" in the design, which will be used to assess trade-offs and to generate recommendations to oil and gas operators.

In order to illustrate the concept, it will be assumed that a simple SCADA system can be represented as shown in Figure 7.

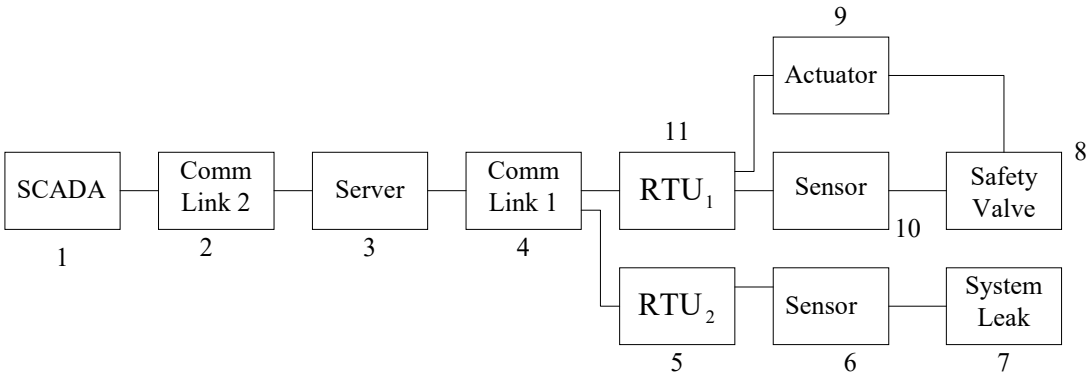

Figure 7. Simple SCADA System

Suppose now we postulate the top event to be a system leak that is not mitigated by action of the safety shut off valve. The fault tree diagram for this system would look like Figure 8.

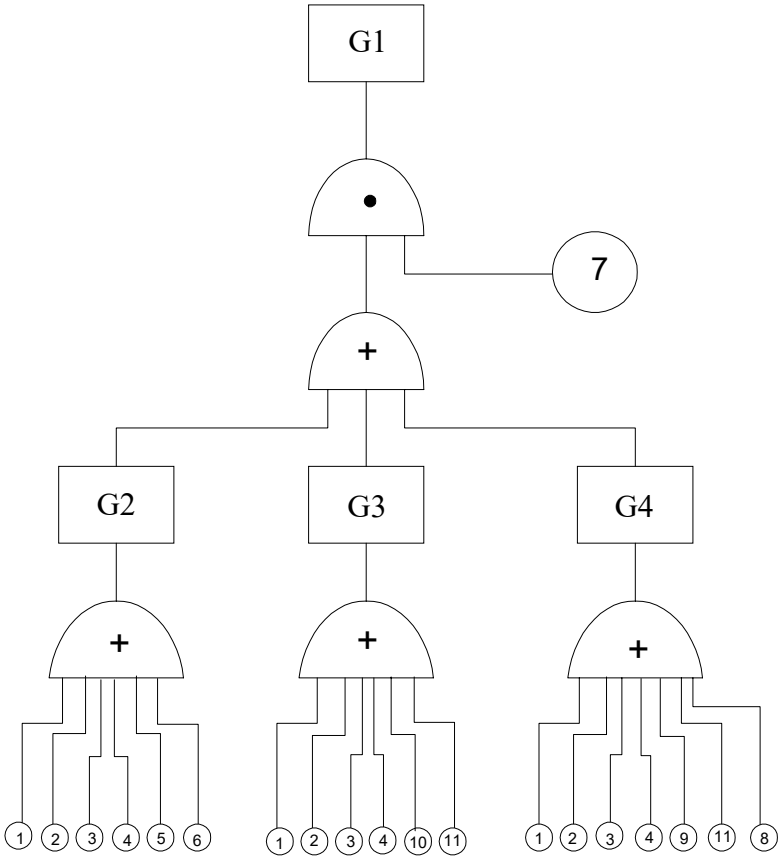

Figure 8. Fault Tree for Simple SCADA System

G1 – Failure to close safety valve in the presence of an oil leak.
G2 – Failure to sense an oil leak.
G3 – Failure to sense state of an open safety valve.
G4 – Failure to close the safety valve.

Basic events –

- q_1 – Failure of the SCADA system
- q_2 – Failure of the communications link 2
- q_3 – Failure of the server
- q_4 – Failure of communications link 1
- q_5 – Failure of RTU_2
- q_6 – Failure of the leak sensor
- q_7 – Failure of the system: an oil leak
- q_8 – Failure of the safety valve to close
- q_9 – Failure of the actuator to close the safety valve
- q_{10} – Failure of the safety valve position sensor
- q_{11} – Failure of RTU_1

This is an example fault tree diagram. If the safety valve is a fail-safe type valve, the state G4 is not a factor. If the SCADA system is designed to close the safety valve regardless of how its state is sensed, then state G3 is not a factor either.

The simplest approach to solving for the availability of the top event is to draw a reduced fault tree. Since the intermediate states G2, G3 and G4 are all the outputs of OR gates and they all feed into an OR gate, the four OR gates can be replaced by a single OR gate with all the basic events, except number 7, as inputs. The new reduced fault tree is as shown in Figure 9.

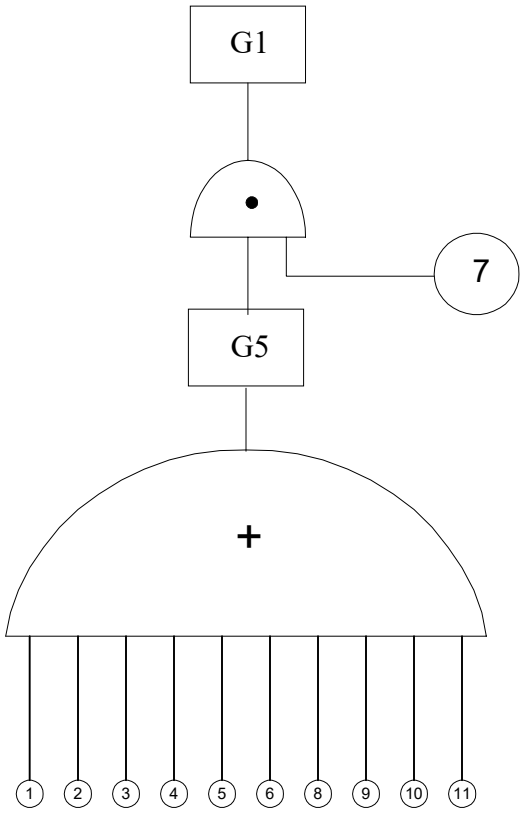

Figure 9. Reduced Fault Tree for Simple SCADA System

G5 - Failure of SCADA system or safety value.

The availability of state G5 is

$$A(\text{top event}) = q_1 A(\text{top event} | q_1 \text{ occurs}) + (1 - q_2) A(\text{top event} | q_1 \text{ doesn't occur})$$

The availability of this top event is

$$A(G1) = q_7 \left[1 - \prod_{\substack{i=1 \\ i \neq 7}}^{11} (1 - q_i) \right]$$

Failure Probability for Hardware Components

The key source of offshore failure data for this study is SINTEF, 1997. Several databases and handbooks exist to help with the estimation of failure probabilities for basic events (Bellcore, 1992; DOD, 1991; Gertman and Blackman, 1994; RAC, 1995). Within the nuclear engineering community, failure data for nuclear-specific systems and components are available from several sources, including summaries of licensee event reports (USNRC, 1980, 1982a, 1982b) and other handbooks (IEEE, 1983; USNRC, 1975).

Development of the Surface/Subsea Fault Tree

The development of the surface system fault tree was built on the Safety Flow Chart-Offshore Production Facility which appears in Figure 10 (Figure 3-1 of the API Recommended Practice 14C, sixth edition, March 1998). The subsea portion of the fault tree was developed using the generalized subsea architecture shown in Figure 4.

The failure rates, repair times and calculated availabilities for the surface system are shown in Table 2. The overall surface fault tree is shown in Figure 11. It should be noted that the failure rates in Table 2 are derived from more detailed drawings of the process equipment and may represent overall subsystems including controls. Most of the failure rates in Table 2 is derived from SINTEF (1997).

The first column in Table 2 contains the event numbers (in the circles) that appear in the fault tree of Figure 11. A short description of the system component that fails occurs in the second column. The third column has the failure rate, in failures per year. This column is derived from the SINTEF (1997) tables, which have the failure rate in failures per million hours. The fourth column contains the time to repair, in repairs per year, and is calculated by dividing the number of hours/year (8760) by the hours/repair from SINTEF (1997). The availability, the last column is obtained by dividing the third column by the sum of the third and fourth columns.

Paste figure here

Figure 10. Safety Flow Chart for Offshore Production Facility (from API RP 14C)

Table 2. Failure Data for Basic Events in Surface System Fault Tree

No.	Basic Failure Events	Failure Rates of Basic Events (Failures per Year)	Repair Times for Basic Events (Repairs per Year)	Availability of Failure
1	TSE (Temp. Safety Element)	0.068	43800	0.0000016
2	ESD (Emerg. Shut Down)	0.092	262.3	0.00035
3	Air			1
4	ASH (Gas Detector)	0.042	1510.34	0.000028
5	Vent	0.18	730	0.00025
6	Containment	0.0004	52.14	0.0000077
7	Containment	0.0004	52.14	0.0000077
8	ESD (Emerg. Shut Down)	0.092	262.3	0.00035
9	PSL (Pressure Safety Low)	0.2	755.2	0.00026
10	FSV (Flow Safety Valve)	2.8	580.13	0.0048
11	LSL (Level Safety Low)	1.01	1108.9	0.00091
12	LSH (Level Safety High)	1.01	1108.9	0.00091
13	Pressure Vessel	0.2	1031.8	0.00019
14	Accident	0.0004	2	0.00005
15	Compressor	4.7	155.87	0.029
16	Pump	2.6	216.3	0.012
17	Heat Exchanger	0.0034	111.88	0.00003
18	Vessel	0.47	842.31	0.00056
19	Valves	2.83	344.88	0.0081
20	Pressure Vessel	0.2	1031.8	0.00019
21	PSH (Pressure Safety High)	0.2	755.2	0.00026
22	PSV (Pressure Safety Valve)	1.95	344.9	0.0056
23	Pump	1.41	217.7	0.0064
24	Flowline	0.0045	612.6	0.0000073
25	Compressor	9.98	135.08	0.069
26	Heat Exchanger	0.018	65.6	0.00027
27	Ventilation	0.18	730	0.00025
28	PSV (Pressure Safety Valve)	1.95	344.9	0.0056
29	Atmospheric Vessel	0.009	842.3	0.000011
30	LSL (Level Safety Low)	1.01	1108.9	0.00091
31	Pressure Vessel	0.2	1031.8	0.00019
32	Atmospheric Vessel	0.009	842.3	0.000011
33	Pressure Vessel	0.2	1031.8	0.00019
34	PSL (Pressure Safety Low)	0.2	755.17	0.00026
35	Ventilation	0.18	730	0.00025
36	PSV (Pressure Safety Valve)	1.95	344.9	0.0035
37	Atmospheric Vessel	0.009	842.3	0.000011
38	Reboiler	0.009	842.3	0.000011
39	FSL (Flow Safety Low)	0.024	14600	0.0000016
40	TSH (Temp. Safety High)	0.068	43800	0.0000016
41	Reboiler	0.009	842.3	0.000011
42	LSL (Level Safety Low)	0.053	1108.9	0.000048

43	TSH (Temp. Safety High)	0.068	43800	0.0000016
44	TSH (Temp. Safety High)	0.068	43800	0.0000016
45	Pressure Vessel	0.2	1031.8	0.00019
46	Compressor	6.1	221.8	0.027
47	Fuel Control	0.07	850.5	0.000082
48	TSH (Temp. Safety High)	0.068	43800	0.0000016
49	TSH (Temp. Safety High)	0.068	43800	0.0000016
50	IPM (Ignition Prev. Measures)	0.042	1510.34	0.000028
51	Flame Emission	0.083	216.3	0.00038
52	PSL (Pressure Safety Low)	0.011	755.17	0.000015
53	Motor Starter Interlock	0.13	216.3	0.0006
54	Spark Emission	8.76	8760	0.001
55	Arrestor	0.0088	365	0.000024
56	BSL (Burner Safety Low)	0.069	1347.7	0.000051
57	Fuel Gas Supply	0.07	850.5	0.000082
58	PSL (Pressure Safety Low)	0.011	755.17	0.000015
59	Air Supply Control	0.083	216.3	0.00038
60	PSL (Pressure Safety Low)	0.011	755.17	0.000015
61	Motor Starter Interlock	0.13	216.3	0.0006

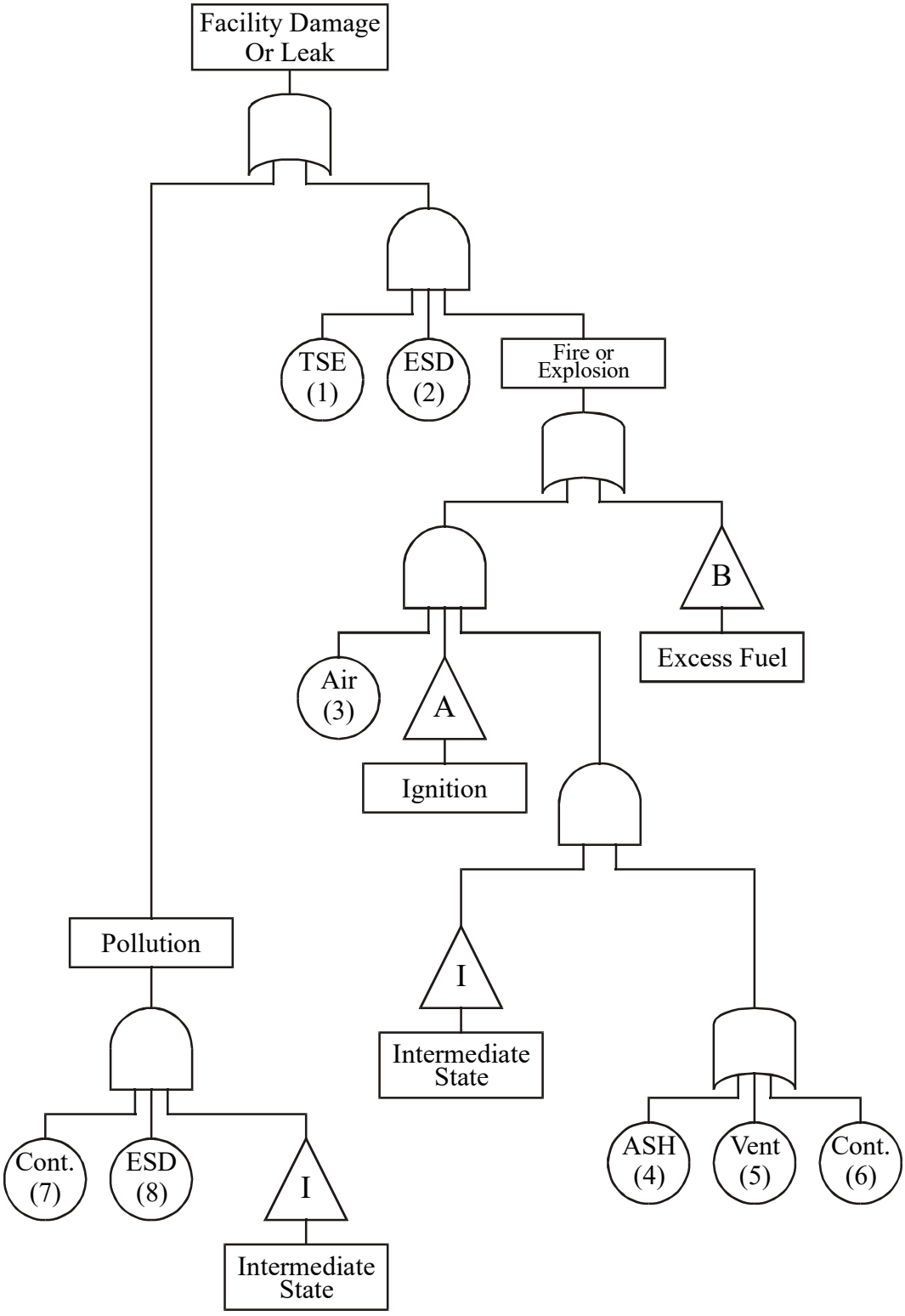

Figure 11a. Top Fault Tree for Damage or Leak

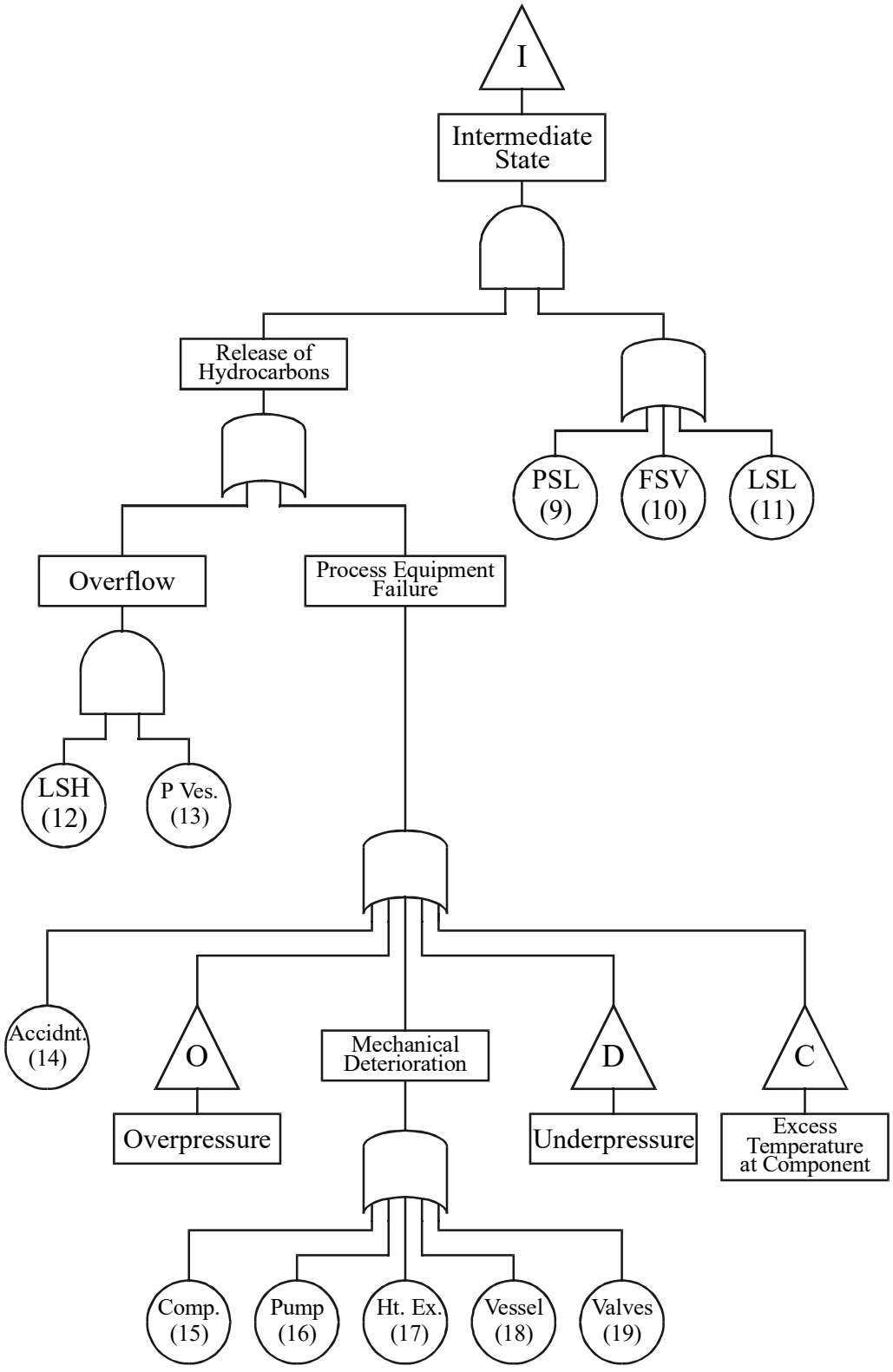

Figure 11b. Intermediate State Fault Tree

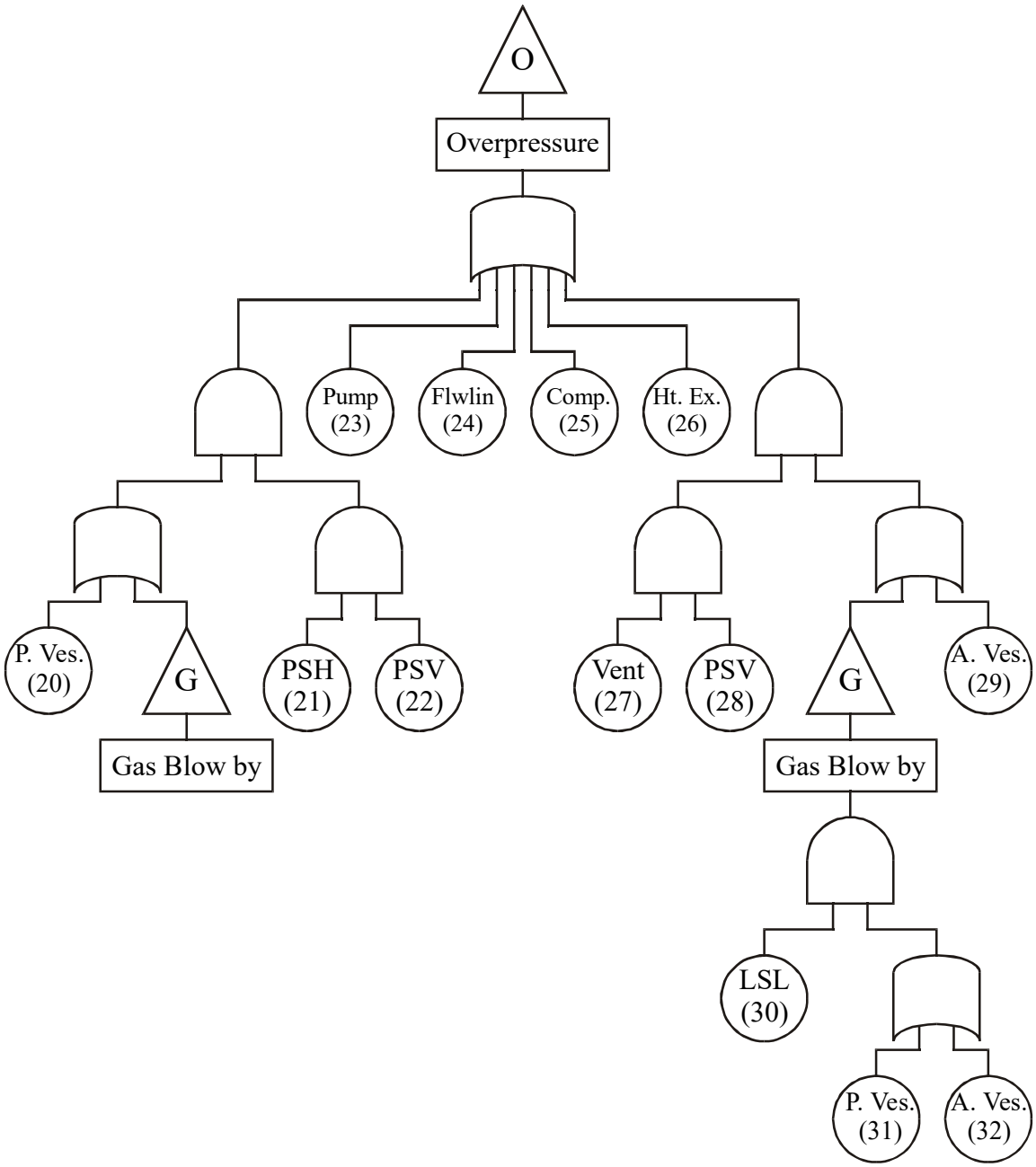

Figure 11c. Overpressure Fault Tree

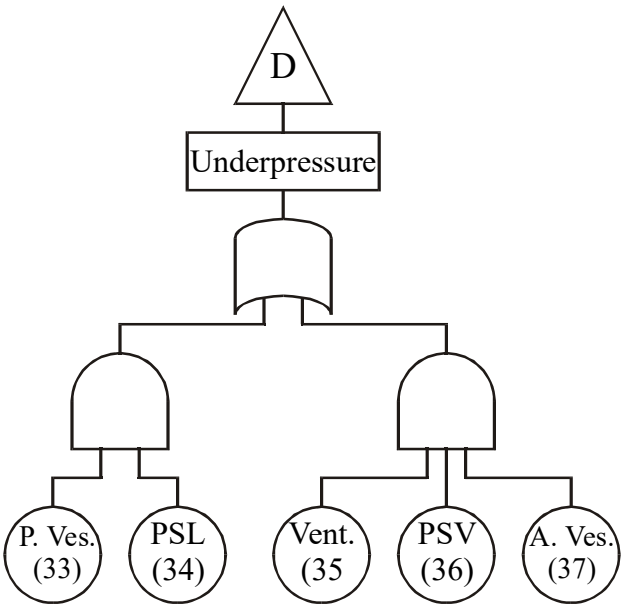

Figure 11d. Underpressure Fault Tree

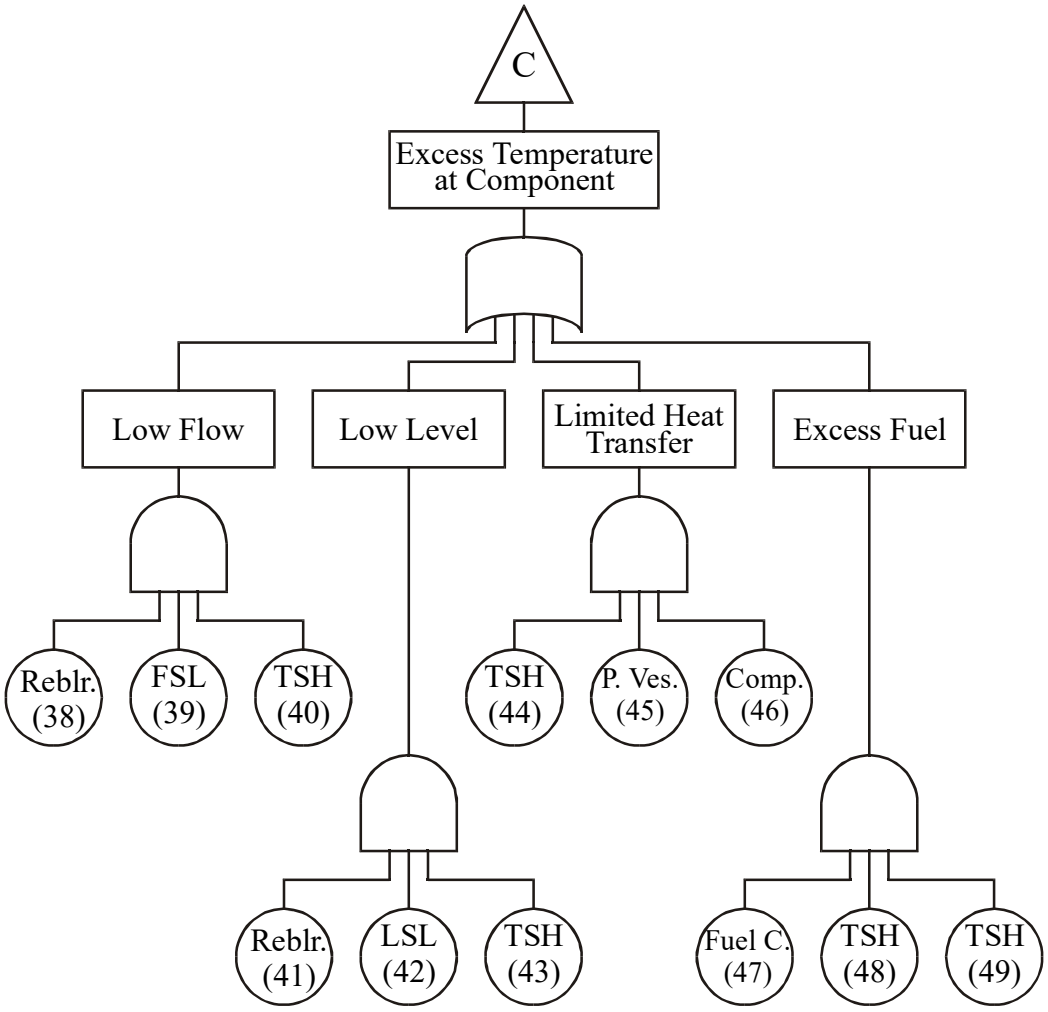

Figure 11e. Excess Temperature at Component Fault Tree

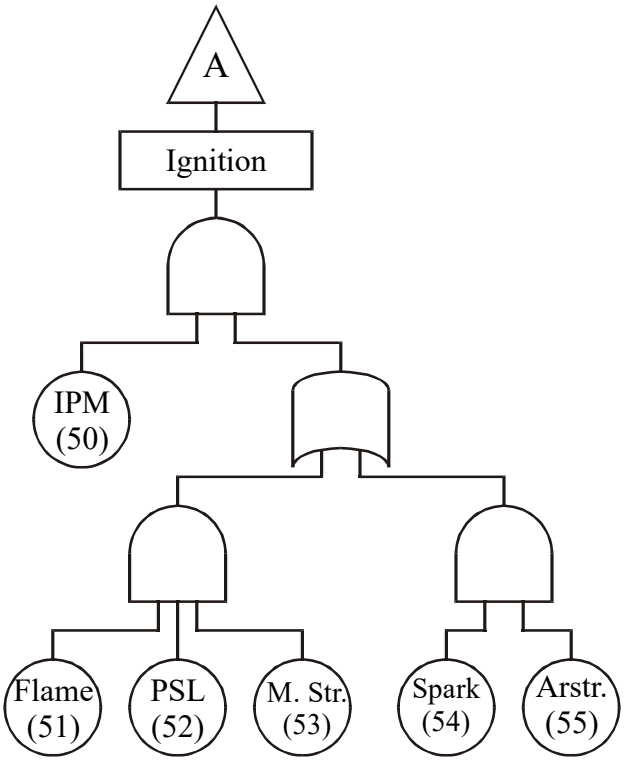

Figure 11f. Ignition Fault Tree

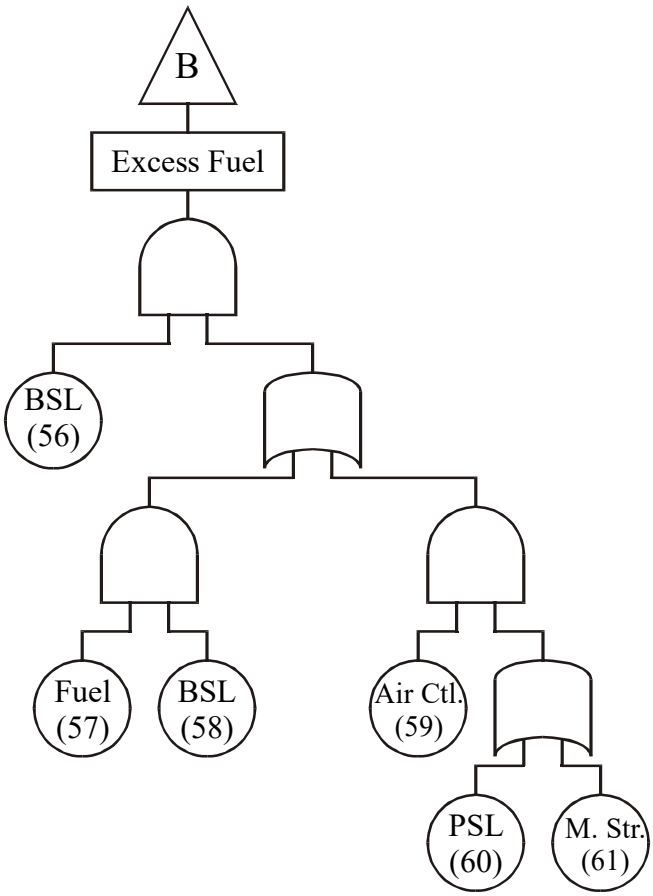

Figure 11g. Excess Fuel Fault Tree

The subsea portion of the fault tree was developed using the generalized subsea architecture shown in Figure 4. The control systems controlling single satellite wells, and more complex subsea production facilities such as multi-well manifold template systems, can be broken into subsystems as shown in Figure 12.

Failure modes for the subsystems shown in Figure 12 include:

Electrical Power Failure - Pod (EFP)
Hydraulic Power Failure - Connector (HFC)
Hydraulic Power Failure - Line (HFL)
Hydraulic Power Failure - Pod (HFP)
Signal Transmission Failure - Connector (SFC)
Signal Transmission Failure - Line (SFL)
Signal Transmission Failure - Pod (SFP)
Signal Transmission Failure - Surface (SFS)

These failure modes are independent events, represented as "OR" gates on a fault tree. Ultimately, however, these "OR" gates are combined because any one fault causes complete system failure.

The block diagram of the subsea control subsystems shown in Figure 12 illustrates the flow of electrical power, hydraulic and communications signals that could lead to a critical failure. It should be noted that this is essentially a series system from a reliability point of view (any failure leads to system failure). There are two areas where redundancy occurs; (1) the redundant subsea control modules at either the well or the subsea manifold, and (2) the redundant PLCs at the host facility. In both cases, the failure of the redundant set is considered the basic event and the failure rate is selected accordingly. With these assumptions, the fault tree will consist of only basic events, "OR" gates and derived states, including the top event.

It should also be noted that three basic events are actually combinations of two or more fundamental events: (1) the electrical power failure of the pod (EFP) could be either a short circuit at the pod connector or a general electric failure in the subsea control unit; (2) the signal transmission failure in the line (SFL) could be either a blocked or plugged sensor or a faulty signal line; (3) the signal transmission failure at the pod (SFP) could be either a pilot valve control failure or a subsystem faulty signal.

Using the block diagram in Figure 12, the fault tree diagram in Figure 13 can be drawn. In this fault tree diagram, hydraulic failures (HFC, HFL or HFOP) and signal failures (SFP, SFC or SFL) can occur for any of the *n* satellite wells. In addition, signal failures on the surface (SFS) can occur for any of the *m* group controls. Once again, the failure rates used account for this fact (Effective failure rate equals *n* or *m* times component failure rate).

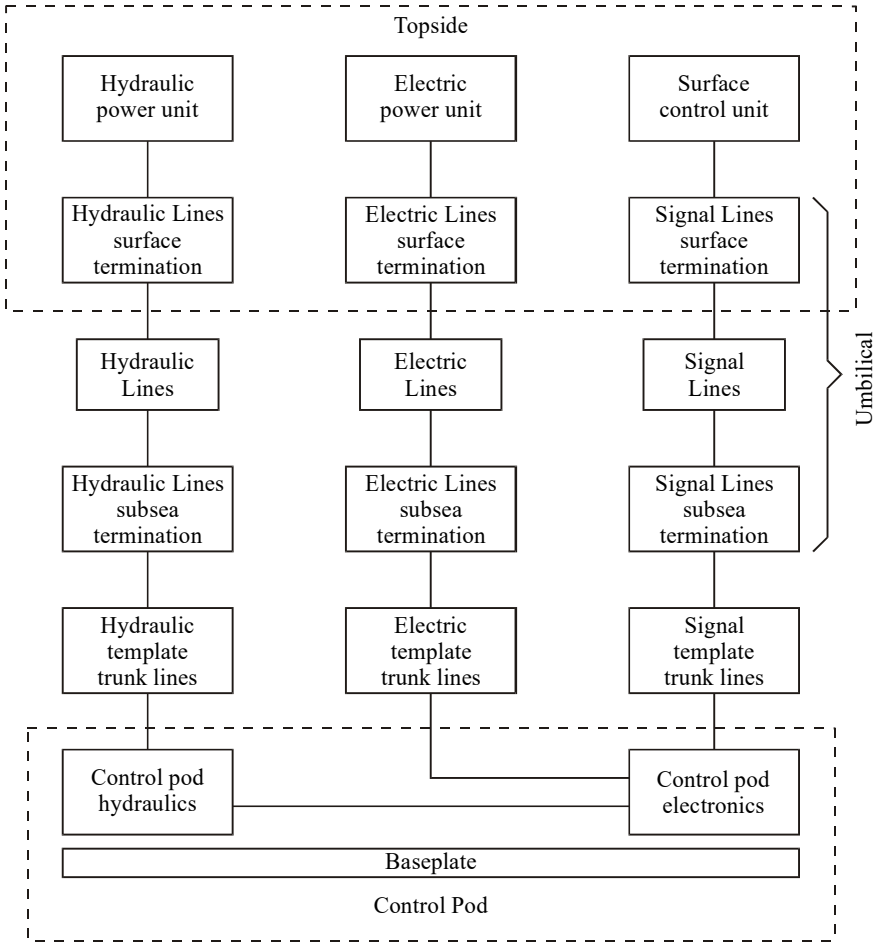

Figure 12. Subsea Control Subsystems

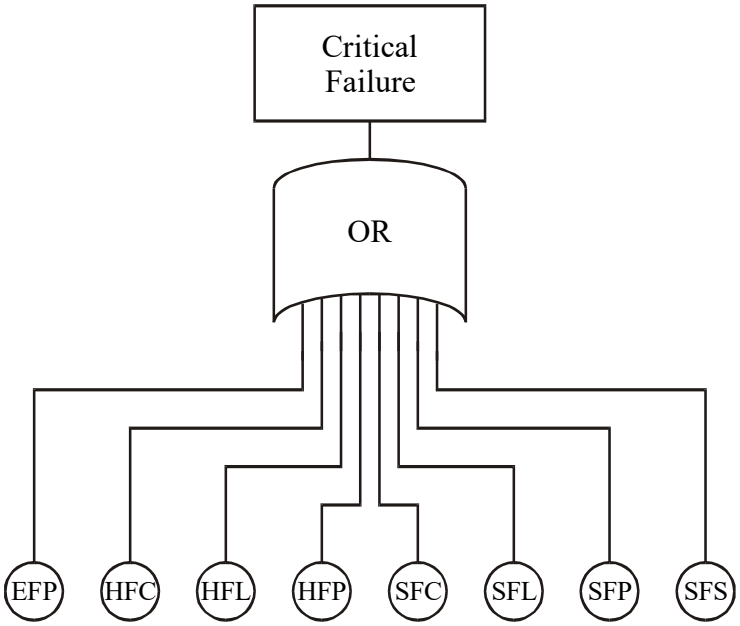

Figure 13. Fault Tree for Subsea SCADA

Based on the data from SINTEF (1997), the following fault rates are used for the basic events in the fault tree:

EFP = 42.8	HFC = 3.81	SFP = 3.81
SFS = 13.69	HFL = 7.62	SFC = 1.90
HFP = 1.90	SFL = 57.4	

where all fault rates are in failures per million hours. It is easily seen that the electric power failure at the pod (EFP) and the signal transmission failure - line (SFL) are the dominant failure modes. The overall failure rate for critical failures is 132.93 failures per million hours or about 1.16 failures per year. This corresponds to a mean time to failure of about 0.86 years.

This failure rate may seem high but, in this context, a "critical failure" means loss of automatic control. Oil spills will also require a simultaneous leak in a critical valve component. This aspect of the reliability study has not been addressed.

Calculating the Availability of the Top Event

Processing the availabilities of component failures through a series of AND/OR gates in a fault tree is a well established process. In general, an AND gate with *n* inputs, each with availability of failure of q_i, results in a new state with availability

$$A(\text{output of AND gate}) = q_i\, q_2 \cdots q_n$$
$$= \left[\prod_{i=1}^{n} q_i\right]$$

In the case of an OR gate the availability of the new state when there are *n* inputs, each with availability of failure of q_i is

$$A(\text{output of OR gate}) = 1-(1-q_i)(1-q_2)\cdots(1-q_n)$$
$$= 1-\prod_{i=1}^{n}(1-q_i)$$

A program capable of performing these operations for a general fault tree without dependent basic events was available and was used to calculate the availability of the top event in these fault trees.

Remember, availability of the top event is the fraction of time a system of components with repair will be in an unsuccessful or failed state.

Non-Independent Basic Events

The above calculation would be rather routine if it were not for the problem of non-independent basic events. The fault tree for the surface system has nine basic events that are repeated. They are failure of:

- Pressure safety valve (PSV)
- Pressure vessel
- Level safety low (LSL)
- Atmospheric vessel
- Ventilation
- Pressure safety low (PSL)
- Temperature safety high (PSH)
- Motor Starter Interlock
- Containment

These particular basic events occur at more than one point in the fault tree. This complicates the calculation because if the basic event occurs at one input with availability of failure, q_i, then it must occur at all other locations with availability of 1. Similarly, if it does not occur at one input with availability 1 - q_i, then it does not occur at all other locations with availability of 0.

Consider a fault tree with one basic event, q_1, that is repeated. The availability of the top event can be found using Bayes Theorem as:

$$A(\text{top event}) = q_1 A(\text{top event} \mid q_1 \text{ occurs}) + (1 - q_2)\, A(\text{top event} \mid q_1 \text{ doesn't occur})$$

The term $A(\text{top event} \mid q_1 \text{ occurs})$ can be found by forcing $q_1 = 1$ and calculating the unavailability of the top event using the fault tree program. In a similar fashion $A(\text{top event} \mid q_1 \text{ doesn't occur})$ can be found by forcing $q_1 = 0$ and using the fault tree program.

When nine repeated basic events occur, the situation is somewhat more complicated. Now one must consider all combinations of these nine events. Since each event can occur or not occur, there are $2^9 = 512$ combinations. In theory, the program should be run 512 times. In reality, one can get a very good approximation by considering only ten of the 512 states. These ten states are the following:

State 1: No basic event failures exist or $q_i = 0$, $i = 1, 9$
State 2 $\rightarrow$ 10: One and only one basic event failure exists or

$$q_1 = 1;\ q_i = 0,\ \ i = 1, 9 \text{ and } i \neq 1$$
$$q_2 = 1;\ q_i = 0,\ \ i = 1, 9 \text{ and } i \neq 2$$
etc.

Then, the availability of the top event will be

$$A(\text{top event}) = \prod_{i=1}^{9} (1 = q_i)\ A(\text{top event} \mid \text{all } q_i = 0)$$
$$+ \sum_{i=1}^{9} q_i \left[\prod_{\substack{j=1 \\ j \neq i}}^{9} (1 - q_j) A(\text{top event} \mid \text{all } q_j = 0 \ \text{ except } q_i = 1) \right]$$

The terms that are neglected all have more than one factor of q_i. Since these terms are small, the product of two or more of these terms is negligibly small.

When the preceding calculation was done for the surface system, a very small availability of the top event resulted (7.6×10^{-13}). This is logical since any path through the fault tree from basic events to top event involves at least four or five failures with availabilities in the 10^{-3} or 10^{-4} range. When these are processed through AND gates, one winds up with $(10^{-3}$ or $10^{-4})^{-m}$ where m is 3 or 4.

The subsea portion of the fault tree is somewhat simpler and represents more of a "series" type system where one or two failures can lead to the top event. Even though individual availabilities of failure are relatively small, because of the nature of the system and its fault tree, the availability of the top event is 0.00618. This corresponds to about 50 hours

of outage per year. In terms of events per year, the top event would have a frequency of 1.16 failures/year.

It should be noted that compressors and pumps have high failure rates and contribute the most to the occurrence of the top event. Containment is also a key since it strongly influences the occurrence of the top event.

Failure of the SCADA System

Figure 14 shows the fault tree for a typical SCADA system as shown in Figure 2. Using failure rates and repair rates, availabilities and unavailabilities can be found for each subsystem. The communication network failure availability is from one operator. The other availabilities are from SINTEF (1997). The availability of the top event (failure of the SCADA system) can be found by analyzing the fault tree diagram with the basic event data of Table 3. Calculating this value results in the availability of the top event (SCADA system failed) equal to 1.2×10^{-2}. Note that the failure rate is dominated by the communication network.

The low availability values for the SCADA system failure and the surface/subsea failure makes it unlikely that these two events could occur simultaneously. The overall availability of a surface/subsea failure and a SCADA failure is about 8.3×10^{-4}. If such an event took an average of one hour to repair, this would lead to a failure rate of about 8300 failures/10^6 hours or about one failure in 1.4 years.

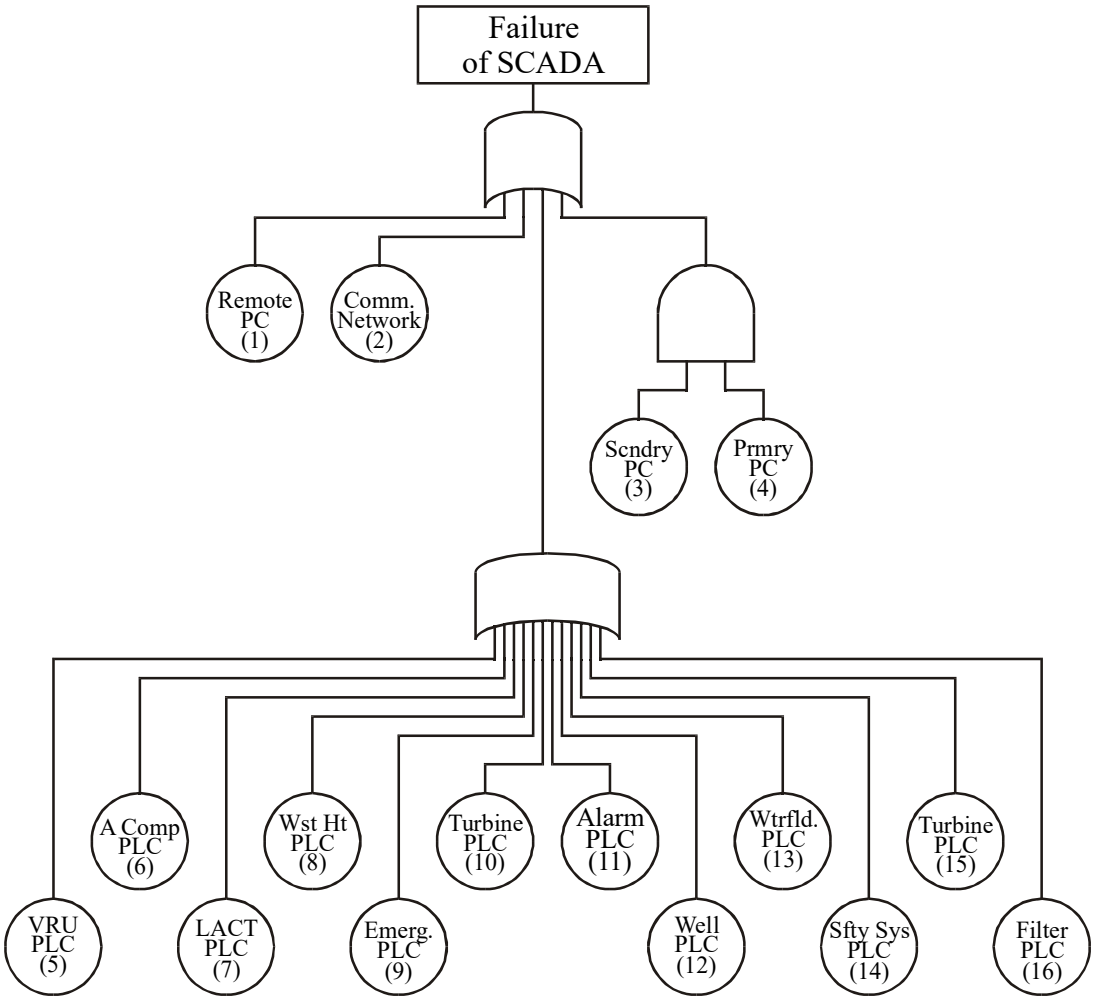

Figure 14. Fault Tree for Distributed Platform SCADA System.

Table 3. Failure Data for Basic Events in SCADA Fault Tree

No	Basic Events	Failure Rates of Basic Events (Failures per Year)	Repair Times for Basic Events (Repairs per Year)	Availability of Failure
1	Remote PC	1.075	2136.6	0.0005
2	Comm. System	109.1	8760	0.01
3, 4	PC	1.075	2136.6	0.0005
5-16	PLC	1.18	7963.6	0.00015

Pipelines

Figure 15 shows the fault tree for a typical offshore pipeline as shown in Figure 5. The corresponding failure rate information is in Table 4.

The pipeline failure rate is from the U.S. Dept. of Transportation (DOT, 2000). In 14 years 2827 failures have occurred. Average pipeline mileage is 154,265 miles. So one can conclude that 14/2827=202 failures per year. By dividing 202 failures/per year by the average mileage we have $1.3*10^{-3}$ failures per year per mile. This number includes both offshore and onshore pipelines. It also includes all types of failures. The failure rate in Table 4 assumes a 30 mile pipeline. The other numbers are from SINTEF, 1997.

For this failure data the probability of the top event (MTBF) is $6.79*10^{-3}$ (failures per year). For the same data the unavailability of the system is $2.67*10^{-2}$. Therefore, the availability of the system is 0.9733.

The SCADA system for a pipeline is generally less complicated than the distributed platform. Nevertheless, we can assume the reliability is probably about the same, since the reliability of the platform system is dominated by the communication system.

Table 4. Failure Data for Pipeline Fault Tree

No	Basic Events	Failure Rates of Basic Events (Failures per Year)	Repair Times for Basic Events (Repairs per Year)	Availability of Failure
1	Press. Sensor	0.01	755	0.117
2	Shut-off Valve	0.03	10950	0.1169
3	Pipeline	0.039	183	0.12
4	Valve	0.11	345	0.026
5	Pump	0.03	322	0.094

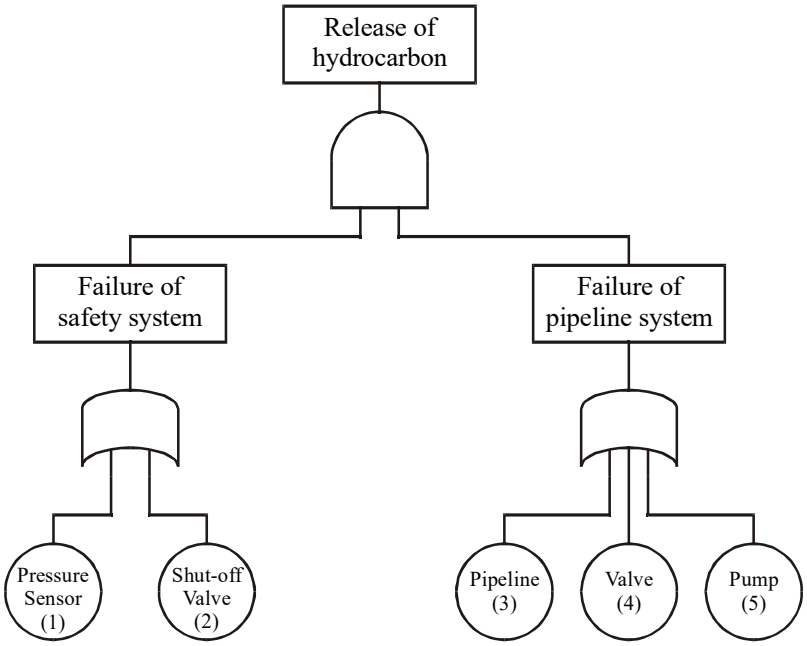

Figure 15. Pipeline Fault Tree.

Human Error

One of the most difficult tasks in a reliability study is to assess the relative importance of human error versus component failures. One of the investigators on this project spent several years applying reliability techniques to electrical safety in underground coal mines. In the course of analyzing historical data on safety it became clear that the majority of fatalities and lost-time injuries resulted from human error. In fact, human error was the source of two thirds of the fatalities and lost-time injuries.

Data exist on the frequency of human error in common tasks found in an industrial environment (Henley and Kumamoto, 1992; Shooman, 1968). The fact that there is a high degree of automation in the operation should minimize the chance of human error.

For the SCADA systems used in offshore platforms, there is not much need for human actions. The SCADA system can fail because of incorrect human action at the remote PC and one of the PLC's, shown as the fault tree in Figure 16. For each PLC, the probability of checking the wrong indicator lamp on the local operator panel is 0.003 (Henley and Kumamoto, 1985). For the PC, the probability of wrongly reading an indicator is 0.001 (Henley and Kumamoto, 1985). Using these numbers, the human reliability in the SCADA system is 0.999964. The human error probability is $1-0.999964=3.54*10^{-5}$.

Since the system is highly automated, the reliability number is considerably relevant.

An area of future study should be to analyze significant failures to determine the relative influence of hardware failures/software failures/human error.

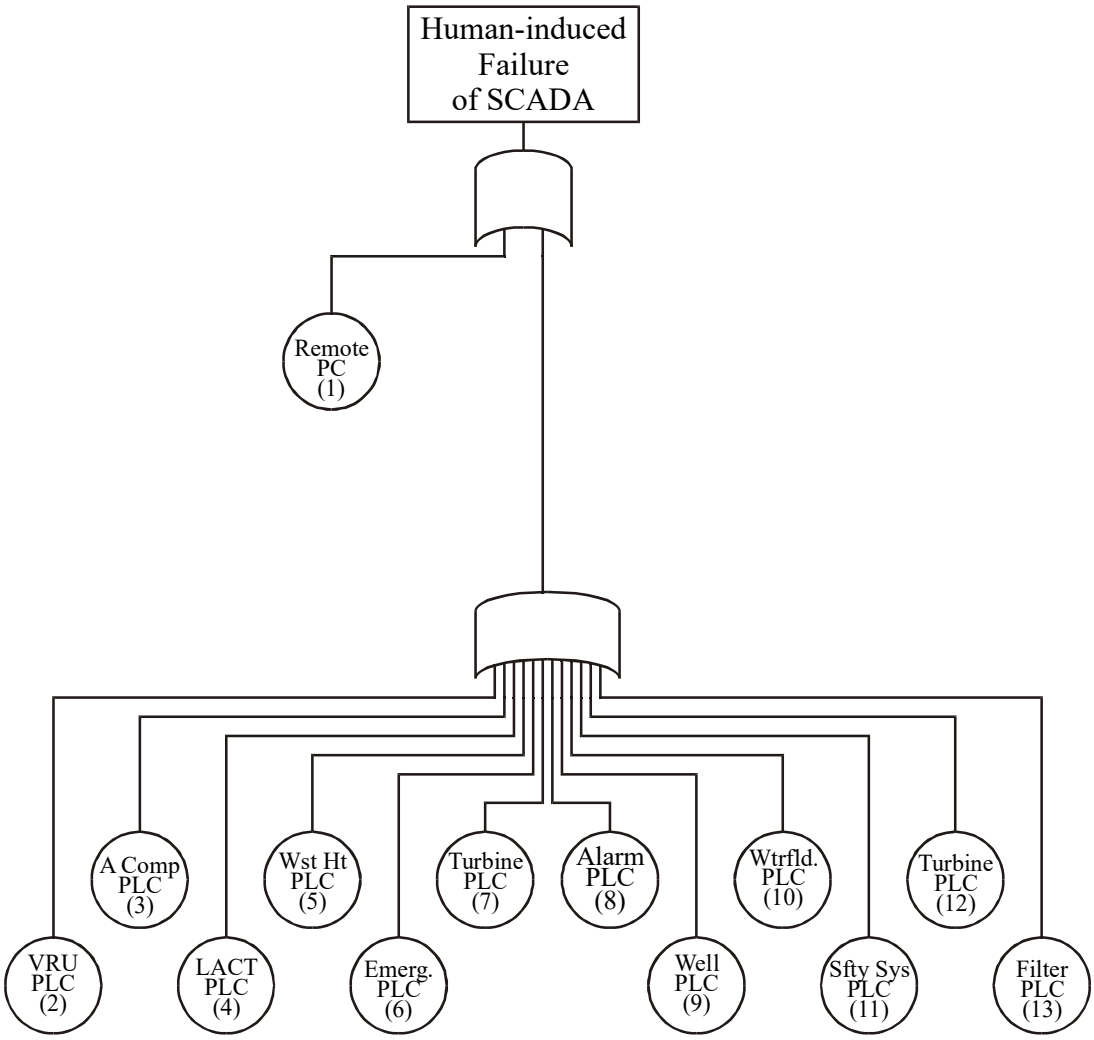

Figure 16. Human-induced SCADA Failure Fault Tree.

Software Reliability

The software reliability was approached in a manner similar to that of the overall SCADA system. The fault tree is the same as for the SCADA system (Figure 14), but with the failure information shown in Table 5.

For each PC in the SCADA system there are 122.66 failures per 10^6 hours. According to OREDA (SINTEF, 1997) 5.61% of these failures are due to software failures. Thus, one

can calculate 6.88 (122.66*5.61 %=6.88) failures per 10^6 hours. The MTTR for PC's is 4.1 hours. From this information, the software availability is calculated as 0.99997.

The failure rate compares in a similar way to digital controllers used in the nuclear industry which have a failure rate of $10^{-7} – 10^{-9}$.

For each PLC, there are 134.83 failures per 10^6 hours. Assuming 5.61 % of these failures are due to software failures, there are 7.56 (134.83*5.61%=7.56) failures per million hours. The MTTR for a PLC is 1.1 hours. From this information, the calculated software availability is 0.99999.

For the routers, the assumption is that 5.61% of the failures are software failures. Communication link availability is assumed to be the same as for the analysis of the entire SCADA system.

The overall availability of the software for the system is 0.9906. As with the previous SCADA system analysis, communication links dominate the calculations.

Table 5. Software-induced Failure Data for Basic Events in SCADA Fault Tree

No	Basic Events	Failure Rates of Basic Events (Failures per Year)	Repair Times for Basic Events (Repairs per Year)	Availability of Failure
1	Remote PC	0.060	2136.6	0.00003
2	Comm. System	109.1	8760	0.01
3,4	PC	0.060	2136.6	0.00003
5-16	PLC	0.066	7963.6	0.00001

Operator Reliability Experience

All of the operators indicated that distant network communications is the weak link in all of their systems. The conversion of analog microwave to a digital microwave network that has a loop architecture has helped in this regard. Nevertheless, the operators program their systems to reliably function even when communications are disrupted.

In the electronic control system, the end devices (sensors, actuators) are the most unreliable parts. The PLC rarely fails. For example, one operator with 200 PLCs had one PLC processor failure in 10 years.

In general, operators were reluctant to share their operational reliability information.

Summary of Reliability Analysis Results

System	MTBF (years)	Failure Availability
Surface	2.5×10^{8}	7.6×10^{-13}
Subsea	0.86	0.00618
Surface/Subsea	0.86	0.00618
SCADA (Platform, Pipeline)	0.09	0.012
Surface/Subsea/SCADA	1.4	0.00083
Pipeline	0.0068	0.027
Human Error	N/A	0.000035*
Software	0.095	0.0094

*human error probability

Software Quality

According to the surveyed operators, software products are selected for offshore platform and pipeline systems based on many of the following features:

- Operating system supported (Windows NT or UNIX)
- Range of supported PLC/DCS/RTU vendors and communication protocols
- Ease of modification
- Intranet Web
- DDE interface
- Alarming
- Historical trending
- Built-in diagnostics

Many of the offshore operators use Wonderware InTouch because it is easy to learn and modify; it also supports a large number of PLC and RTU vendors. Rockwell Software is another leading vendor. Others include Intellution, Siemens, GE Fanuc, and CiTech. In addition, users and third parties often develop interfaces for special or obscure equipment.

Vendors and operators are always reluctant to share defect data; software companies are no different. Thus, in order to gain an alternate appreciation of software quality and reliability, we also chose a qualitative and more subjective approach. We requested an interview of the major software vendors to discuss their software development and maintenance processes, including quality assurance (QA). We assured them that no comments would be attributed to a specific source but that we whould share summary information and highlight best practices, again in a non-attributional fashion. A questionnaire was developed based on the Software Engineering Institute's Software Capability Maturity Model (Humphrey and Sweet, 1987) and on industrial software supplier evaluation processes (Nielsen and Miller, 1996). The questionnaire was provided

to the vendors prior to the interview. The complete questionnaire is included in Appendix A.

Software Survey Results

Software products included control software and human-machine interface software. Typically, development teams are small in size and focus on a particular aspect of the total software package. The total software products are large (1.5 – 2 Million Lines of Code).

The following contains a list of best practices and a list of deficiencies which were found. No single company performed all of the best practices; no single vendor had all of the noted deficiencies. Those software development teams with established engineering roots in the company seem to have the best processes. Smaller software-only companies tend to have less well-defined processes and operate more on an ad hoc basis. However, as those companies addressed the issue of multiple releases and long-term maintenance, they have instituted additional processes and some have utilized third-party vendors for maintenance and configuration management.

Best practices noted among the interviewees were:

- A defined software process that is utilized throughout the organization. The process does not need to be cumbersome or labor-intensive; in fact, some of the best were quite streamlined; the important aspect is that the process was consistently applied. Training in the process for new hires was also noted as a best practice.
- Migration to a common software infrastructure. Several of the vendors are developing a framework into which existing components (either in-house or from other vendors) can be "plugged." This allows for shared components, reducing development time and redundancy of information.
- Frequent solicitation of customer input, requirements, and satisfaction through well-defined channels. The best vendors had a formal mechanism by which they could learn of new customer expectations as well as problems and issues.
- On-line sites for customer access of updates, issues, and information. Many have websites for customers. One vendor moderates a website in which customers provide feedback and carry discussion threads on various topics of interest.
- Software teams which included staff with industrial experience using SCADA equipment (the highest percentage found was 15%). These individuals tended to serve as application engineers and product architects, rather than as programmers or testers.
- Reviews at various phases of development that include participants from other development teams as well as test and QA.
- Previews or "look-ahead" meetings that bring together software architects and application engineers to determine risks and potential pitfalls of next phase of development.
- Concern for documentation ease of use by customer/operator.
- Independent test teams with separate reporting relationship from development team.

Deficiencies noted include:

- Ill-defined software development processes or multiple processes that vary from team to team.
- Conducting reviews in which not all parties have examined the material in advance or in which not all perspectives are present.
- Lack of formal regression testing procedures and test suites.
- Lack of emphasis on failure scenario tests.
- Lack of concern for intrusion detection capability.

Lastly, while vendors stated that they had requirements for safety, reliability, quality, and real-time operation, no one shared specific quantifiable requirements. This is an area for further exploration.

Recommendations

Based on the reliability assessment of current SCADA technology, we propose the following additional guidelines for those operators that use SCADA systems. These are in addition to the guidelines in NTL N00G06 (effective February 4, 2000).

- All developed software for SCADA systems should follow a defined software process; that process does not necessarily need to be an SEI or ISO or IEEE standard, although those may be applicable. This recommendation applies both to software developed by the vendors and application-specific software developed by the operators/vendors/contractors.
- Software should also be tested for survivability under typical intrusion mechanisms, such as buffer overrun. If the software contains embedded third-party components, those components should be thoroughly tested within the total system. This includes testing of "negative requirements," that is, testing of features of the embedded component that should not be activated in the larger framework.
- Critical parts of the system, such as the emergency shutdown system, should be redundant. For subsea systems, the communication channels should be redundant.

Other recommendations:

- MMS should organize a project to collect failure data that is not covered by current SINTEF projects. Specifically, operators in the OCS of North America should be surveyed to collect data on pneumatic safety systems, pipeline system components and human operators. This project should be organized like the SINTEF projects.
- MMS should survey offshore platform operators concerning their long-term plans about remotely operating offshore platforms from the shore.
- MMS should require a reliability assessment of complete subsea processing systems.

References

API, 1998. *Recommended Practice 14C*, sixth edition, March 1998; Recommended Practice for Analysis, Design, Installation, and Testing of Basic Surface Safety Systems for Offshore Production Platforms.

ARC Advisory Group. 1999. *Oil & Gas, Water SCADA Systems Global Outlook*, ARC Advisory Group, Dedham, MA, 3/99.

Bellcore. 1992. *Reliability Prediction for Electronic Equipment*, Report TR-NWT-000332, Issue 4, September.

Billinton, R. and R.N. Allan. 1992. *Reliability Evaluation of Engineering Systems: Concepts and Techniques*, 2nd Ed., New York: Plenum Press.

DOD (U.S. Department of Defense). 1991. *Reliability Prediction of Electronic Equipment*, Mil-Handbook-217F. New York: Griffiss Air Force Base. December.

DOT (U.S. Department of Transporation) Office of Pipeline Safety. 2000. *Pipeline Statistics*, Web page address: http://ops.dot.gov/stats.htm

Gertman and Blackman. 1994. *Human Reliability and Safety Analysis Handbook*, New York: Wiley.

Henley, E.J. and H. Kumamoto. 1985. *Designing for Reliability and Safety Control*, New Jersey: Prentice-Hall Inc.

Henley, E.J. and H. Kumamoto. 1992. *Probabilistic Risk Assessment*, New York: IEEE Press.

Humphrey, W. and W. Sweet. 1987. *A Method for Assessing the Software Engineering Capability of Contractors*, Tech. Report CMU/SEI-87-TR23, Pittsburgh : Software Eng. Inst.

IEEE (Institute of Electrical and Electronics Engineers). 1983. *IEEE Guide to Collection and Presentation of Electrical, Electronic and Sensing Component and Mechanical Equipment Reliability Data for Nuclear Power Generating Stations*, Std 500-1984, New York: IEEE.

ISA (Instrument Society of America). 1998. “SCADA Software Roundup,” Industrial Computing, 17, 18-37, October.

Mitchell, C.M. and K. Williams. 1993. “Failure Experience of Programmable Logic Controllers Used in Emergency Shutdown Systems,” *Reliability Engineering and System Safety*, 39:329-331.

Musa J.D., A. Iannino, and K. Okumoto. *Software Reliability: Measurement, Prediction, Application*, McGraw-Hill, 1987

Neilsen, J. and A. Miller. 1996. "Selecting Software Subcontractors," *IEEE Software*, 104-109, July.

Paula, H.M. 1993. "Failure Rates for Programmable Logic Controllers," *Reliability Engineering and System Safety*, 39:325-328.

Paula H.M., M.W. Roberts, and R.E. Battle. 1993. "Operational Failure Experience of Fault-tolerant Digital Control Systems," *Reliability Engineering and System Safety*, 39:273-289.

Paulk, M., B. Curtis, M. Chrissis, C. Weber. 1993. *Capability Maturity Model for Software, Version 1.1*, Tech. Report CMU/SEI-93-TR-24, Pittsburgh : Software Eng. Inst.

RAC (Reliability Analysis Center). 1995. *Nonelectronic Parts Reliability Data 1995*, Rome, N. Y.: Reliability Analysis Center.

Shooman, Martin L., *Probabilistic Reliability: An Engineering Approach*, McGraw-Hill, New York, 1968.

SINTEF, 1997, *OREDA - Offshore Reliability Data*, 3rd Edition, SINTEF Industrial Management, Trondheim, Norway.

USNRC (U. S. Nuclear Regulatory Commission). 1975. *Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Plants*, NUREG-75/014, USNRC Report WASH-1400, Washington, D.C.: USNRC, October.

USNRC. 1980. *Data Summaries of Licensee Event Reports of Diesel Generators at U.S. Commercial Nuclear Plants*, NUREG/CR-1362, Washington, D.C.: USNRC, March.

USNRC. 1982a. *Data Summaries of Licensee Event Reports of Pumps at U.S. Commercial Nuclear Plants*, NUREG/CR-1205, Washington, D.C.: USNRC, January.

USNRC. 1982b. *Data Summaries of Licensee Event Reports of Valves at U.S. Commercial Nuclear Plants*, NUREG/CR-1363, Washington, D.C.: USNRC, October.

USNRC. 1993. *Software Reliability and Safety in Nuclear Protection Systems*, NUREG/CR-6101, Washington, D.C.: USNRC.

Wheeler D.A., B. Brykczynski, and R.N. Meeson (eds.). 1996. *Software Inspection: An Industry Best Practice*, New York: IEEE Press.

Appendix A

SCADA SOFTWARE QUESTIONNAIRE

University of Missouri – Rolla
for
Department of the Interior, MMS
Technology Assessment and Research Program SOL 14335-01-99-RP-3995

Survey Participants:

Senior Executive (30 minutes)
SCADA product development manager (60 minutes)
SCADA product marketing manager (60 minutes),
QA manager or a QA engineer (60 minutes),
Team meeting with a developer, a tester, and a configuration manager (60 minutes).

Questions:

General Management

What is the vision of the company?
How do the communications, control and SCADA products fit within the company's product line?
With regard to communications, control and SCADA applications, does the company produce software only or systems of software and hardware?
What levels of the organization have direct customer contact?
If individuals do not have direct customer contact, who internally serves as their customer interface? Who internally serves as customer advocate?
How is customer satisfaction measured? (all measures that apply)

SCADA Software Process Information: Personnel

What is the size of the software team? What percentage are developers? Testers? Other team members?
How many have had industrial experience using SCADA equipment? (Numbers or percent of total)
What training is provided to new hires? (General and/or SCADA-specific)
Is there an annual training goal? Is it a mandate, an opportunity, or something in between?
Is there a training course or program for new managers? If so, what topics?

SCADA Software Process Information: Requirements and Configuration Management

How are customer requirements determined?
How are product requirements determined?
What quantifiable requirements exist for Safety? Reliability? Quality? Real-time Operation?
How are requirements tracked throughout the product development life cycle?
How are releases determined and how is functionality assigned to releases?
How are releases managed?
How are customer-reported defects fixed? (Work-around patches and/or new releases)

SCADA Software Process Information: Development

What automated tool support is used?
Is any of the communications/control/SCADA software externally supplied? If so, subcontract development or COTS product?

SCADA Software Process Information: Test and Quality Assurance

What internal reviews and audits are regular activities? (SEI CMM, ISO, etc.)
What standard reviews and audits are regular activities? (SEI CMM, ISO, etc.) For each of these, what is the periodicity of review/audit?
How are defects identified, fixed, tracked and verified?
Is the test team independent of the development team?
What is the reporting relationship of the test team relative to the development team?
What levels and types of testing are performed?
How are fail-safe requirements, if any, tested?
How are real-time requirements, if any, tested?
Who approves product release/shipment? On what basis?
If a customer purchases your software product, what, if any, are the stated liabilities?