APPENDIX A

EXAMPLE CHECKLIST OF DEVICES TO BE CHECKED FOR YEAR 2000 COMPLIANCE FOR AN EXAMPLE CHEMICAL PLANT

APPENDIX A
EXAMPLE CHECKLIST OF DEVICES TO BE CHECKED FOR YEAR 2000 COMPLIANCE FOR AN EXAMPLE CHEMICAL PLANT

COMPONENT (to check for compliance)	Worst Case Failure Effects
Embedded Microchips	
Controllers	
Weighers	In accurate readings resulting in poor conversion
Reactor	
Charging	Wrong amounts reacting-poor conversion
Temperature	Poor conversion-explosion
Pressure	Poor conversion-explosion
Cleaning	Inaccurate timing-process interruption-release
Stripper	Contamination of product
Dryer	Water contamination of product
Centrifuge	Poor separation
Storage	Overflow-release
Video Cameras	Failure to work
Still Cameras	Failure to work
Alarm Systems	Failure to work
Clocks	Show incorrect time
Elevators	Failure to work
Phones	Failure to work
Answering Machines	Failure to work
Software	
Main frame, network, desktop, & communication computers	Data generated errors may result in inaccurate data or system failures
Office computers	
Purchasing	No supplies
Inventory	Excess supplies
Distribution	Will send out incorrect orders
Sales	Will not be able to keep up with orders
Accounting	Will compute incorrectly
Personnel	Will not be kept up correctly
Process Computers	
Control	Explosion-release
Transportation	Buildup of stock
Quality Control	Poor quality

APPENDIX A
(continued)

COMPONENT (to check for compliance)	Worst Case Failure Effects
Supply Chain	
Utilities	
Electricity	Process shut down
Water	Process shut down
Waste	Waste buildup beyond capabilities
Communications	No communication
Raw material suppliers	
Primary feedstock	Process shut down
Initiator-catalyst	Process shut down
Service providers	
Insurance	Extra expenses
Hospitals	No medical care
Vending	No food
Customers	No incoming funds
Security	
Video cameras	Failure to work
Security lights	Failure to work
Access	
Parking	Failure to work
Building	Failure to work
Room	Failure to work
Alarms	
Fire	Failure to work
Intrusion	Failure to work
Warning	Failure to work
Process	Failure to work

Note: The information given in this table is provided as an example only. Checklists like this should be developed on an individual plant-specific basis using criteria and knowledge that are unique to the plant.

APPENDIX B

PRESENTATION ON YEAR 2000 COMPLIANCE EFFORTS BY OXYCHEM GIVEN AT THE EXPERT WORKSHOP CONVENED BY THE U.S. CHEMICAL SAFETY AND HAZARD INVESTIGATION BOARD AT THE REQUEST OF THE SENATE SPECIAL COMMITTEE ON THE YEAR 2000 TECHNOLOGY PROBLEM*

*** Also available as an audio presentation at**
http://www.chemsafety.gov/1999/news/n9907.htm

Occidental Chemical Y2K Program

Occidental Chemical's Y2K Program Focuses on Five Key Areas:

Information Technology

Control Systems

Suppliers

Customers

Contingency Planning

Occidental Chemical Y2K Program

Each and Every Area of the Y2K Program depends on a process that includes the following steps:

Inventory

....or identification of all the devices, systems or relationships where there is a concern about Y2K failures.

Investigation

....or determining the true likelihood of failure and the impact should a failure occur.

Remediation

....or actions that will correct the Y2K related deficiency or mitigate the impact of a failure.

Documentation

....or creation of information needed to share results and show due diligence.

When focusing on Process Plant Safety, the two most important parts of the Y2K Program are:

IT

Control Systems

Suppliers

Customers

Contingency Planning

Control Systems

...or the process being used to identify and correct the problems associated with microprocessors and programming that is embedded in systems and devices used to monitor and control process plants.

Contingency Planning

...or the process being used to identify the likely scenario and make plans to deal with it AND to surface possible situations and to ensure ability to respond to them.

Occidental Chemical Y2K Program

Handling Control Systems includes the following elements:

Inventory

- Identify ALL systems and devices containing microprocessors and programming.
- Prioritize all identified items according to both "likelihood" of failure and "Impact" should a failure occur.

Investigate

- Create a standard methodology for investigating devices - Include:
  - Triage by priority - eliminate low/low items
  - Shared Information - eliminate items screened elsewhere
  - Vendor Information - eliminate items vendors have tested and confirmed to be compliant or not a Y2K device.
  - Physical Inspections - Battery or Digital vs. Analog signals
  - Details Testing - Rigorous preparation and execution
- Create Database to Record Results and Share Information
  - Think about end results before starting Database design
  - Don't spend all your time working on the "means to the end"
- Provide Adequate Technical Support. While not a particularly technically demanding issue, there are some important subtleties about Y2K.
  - Clock cycle issues
  - Integration and Inter-relationships
  - Overall process flow - Focusing in on the right things.
  - Y2K Issues that will not occur in the year 2000 or integrating Y2K thinking in everyday business.

Handling Control Systems (continued):

Remediate

- Create a standard methodology to streamline getting things done.
  - Don't try to be opportunistic .... fix the Y2K problem
  - Take patches and fixes supplied by vendors
  - When a vendor doesn't have a plan .... fire up the steam roller
  - This is not the time for normal budget cycles
- Track remediation to ensure closure
- Test after remediation

Document

- Create a minimum standard requirement for documentation
  - Describe What, Who, When, Where
  - Don't duplicate
  - Audit while work is being done

Occidental Chemical Y2K Program

Addressing Contingency Planning includes the following elements:

Preparing for the "Most likely worst case scenario."

- What is the likely scenario for IT Systems?
- What is the likely scenario for Control Systems?
- What is the likely scenario for suppliers?
- What is the likely scenario for close-linked customers and other customers?
- What is the likely scenario for for the surrounding community?
- Create a "composite" scenario. Assume that multiple problems occur simultaneously.
  - Conduct "What-if" exercises
  - Conduct Table Top exercises

Preparing for Emergency Response.

- Identify "Unlikely" situations.
- Identify "Unrecognized" situations.
  - You know where your focused your attention.
    - What did you take for granted?
- Identify recognized situation you have been "Unable to address".
- Test Emergency Response capacity in addressing situation described above.

Successful Y2K programs will incorporate the following characteristics:

Project Management

- Upon his arrival at the Death Star, where construction was behind, Darth Vader's entering line was "I'm here to put you back on schedule." You'll need a Darth Vader.

Process Development

- No one has ever addressed Y2K before .... and it doesn't come naturally. You'll need someone who understands and can articulate how the process will work in a plant.

Process Implementation

- There have been billions of dollar and million of man-hours spent on process re-design in the last ten years ---- go find one that is working as intended. You'll need someone who can get things functioning as designed across a wide variety of sites.

Accountability/Authority

- Y2K is one of those things most people would like to see just go away .... it won't go away. You'll need to point at someone and say "It's your job." That person will need the resources to do his or her job.
- Normal methods of resource allocation will hinder progress. You'll have to decide if you can stand the delays.

Occidental Chemical Y2K Program

Occidental Chemical's Y2K Contingency Program Has Three Main components:

Contingency Level 1:

Continued Safe Operations

Contingency Level 2:

Safe Shut Down

Contingency Level 3:

Emergency Response

Contingency Level 1: Continued Safe Operations

Those things necessary to keep the facility operating in a safe and environmentally sound manner...

Should the Y2K Program Steps fail to prevent a problem, ...

what pre planned actions can be taken that would allow the facility to continue operations safely and in an environmentally sound manner?

Occidental Chemical Y2K Program

Contingency Level 1: Continued Safe Operations Examples

- Minimize finished product inventories and waste/effluent levels to allow as much reaction time as possible to unusual situations
- Maximize raw material inventories (within safe limits) in case your supplier fails
- If you purchase a small amount of steam, you should consider renting a mobile steam generator for back up should your supplier fail
- "Ditto" for air or nitrogen with bottled gas for back up
- Consider low tech/cheap walki-talkies to back up sophisticated communication systems

Contingency Level 1: Continued Safe Operations Examples (Cont.)

- Increase operations & craftsman staffing during critical periods to be able to quickly respond to unusual situations
- Shut down non essential units; restart them later after critical periods have passed and essential units are running well
- Make pre arrangements with trucking firms to handle material if primary transportation modes are not available
- Develop a plan to manually control output from variable frequency drive controllers (switch to fixed speed and control volume output via dampers, valves, etc.)
- Identify and test manual overrides for security systems

Occidental Chemical Y2K Program

Contingency Level 2: Safe Shut Down

Those things necessary to shut the facility down in a safe and environmentally sound manner...

Should the Y2K Program Steps fail to prevent a problem, and the Contingency Level 1 plans fail to keep the facility operating safely, ...

what pre planned actions can be taken that would allow a safe and environmentally sound shut down of the facility?

Contingency Level 2: Safe Shut Down Examples

- Rent portable electrical generators or lights for emergency use
- Icrease operations & craftsmen staffing during critical periods to monitor and react quickly for shut down purposes
- Shut down non essential equipment before critical periods to allow more attention time for shut down of critical systems
- Ensure (test) all emergency shut down equipment and safety systems are fully functional before critical periods
- Test UPS back up systems to ensure power is supplied to control systems that allow safe shut down

Occidental Chemical Y2K Program

Contingency Level 2: Safe Shut Down Examples (Cont.)

- Consider having a back up low tech. communication system for use in plant if the main system fails
- Pre test emergency vent scrubbing systems to eliminate or minimize emissions during shut down
- Conduct S/D drills--consider more than one system failure

Contingency Level 3: Emergency Response

Those things necessary for an adequate and proper emergency response to facility incidents...

Should the Y2K Program Steps fail to prevent a problem, and the Contingency Level 1 plans fail to keep the facility operating safely,

and the Contingency Level 2 plans fail to shut the facility down safely, ...

what pre planned actions can be taken that would ensure adequate and proper emergency response to facility incidents?

Occidental Chemical Y2K Program

Contingency Level 3: Emergency Response Examples

- Consider having the Plant Emergency Response Team on "Active" stand-by
- Work with "outside" responders and pre plan a back up communication mechanism and practice a response plan
- Develop a system to warn neighbors in case the local emergency warning system fails
- Conduct drills considering multiple system failures
  - Internally
  - With "outside" response agencies

APPENDIX C

PRESENTATION ON YEAR 2000 COMPLIANCE EFFORTS BY ROHM AND HAAS GIVEN AT THE EXPERT WORKSHOP CONVENED BY THE U.S. CHEMICAL SAFETY AND HAZARD INVESTIGATION BOARD AT THE REQUEST OF THE SENATE SPECIAL COMMITTEE ON THE YEAR 2000 TECHNOLOGY PROBLEM*

*** Also available as an audio presentation**

http://www.chemsafety.gov/1999/news/n9907.htm

Chemical Process Safety and the Year 2000

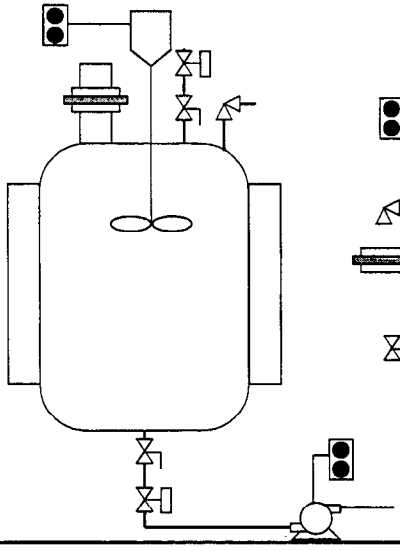
- Basic process control safety
- The implications of Y2K
- Program overview
  - Scope
  - Requirements
- Findings
- A final layer of protection

The Layers of Protection in a System

- Any physical device can - and **will**, at some point - fail
- Systems must be designed to withstand failures
- Failure protection is layered:
  - Basic equipment protection
  - Basic control system architecture
  - Fail-safe design
  - Operators and engineers
  - Administrative procedures

Increasing Robustness

Basic Equipment Protection Layer



Local motor control

Pressure relief devices

Manual shut-off valves

Basic Control System Architecture Layer

Operators are an important line of defense

Increasing likelihood of date dependence

Corp. Sys. — Scheduling, e.g. Several layers of protection beneath.

Isolation

Supervisory — Typically PC or DCS. Operations should run, or fail safely, if this fails.

Regulatory — Typically PLC or DCS. If PLC, typically date-impervious.

Hardwired — Safety interlocks and ESD. Typically relays or date-impervious PLC.

Field Equipment. Typically date-impervious.

Fail-Safe Design Layer

- Systems are designed to fail safely
- Facilities and control systems are designed to withstand the loss of:
  - Process and control devices
  - Power
  - Water
  - Other utilities
- All systems are subject to formal design reviews:
  - HAZOP
  - Failure modes and effects analysis
- System design emphasizes ability to achieve safe shutdown

The Implications of Year 2000

- Systems and processes are designed to deal with single failures
- Year 2000 could cause multiple concurrent failures
  - Control failures
  - Utilities
- Safe design and a Year 2000 program provide good protection against multiple control failures
- Greatest exposure is in utility failures

Rohm and Haas Corporate Policy

Rohm and Haas Company is committed to identifying and correcting date-based problems in computer systems (hardware and software), commonly referred to as the "Year 2000 Problem", so that all critical operations continue without disruption.

This policy applies to all Company units, world-wide, including subsidiaries, joint ventures, and other related units.

Rohm and Haas Scope

- Business computer systems
- Technical infrastructure
- End-user computing
- Customers and suppliers
- **Manufacturing and warehousing**
- **Environmental**
- Research and development
- Other

Two Classes of Manufacturing Systems

- Process control systems
- Other physical systems

- Similar approach for both
- Slightly different requirements for each class
- Both efforts coordinated by same group

Control Systems Scope

Computer-based equipment that directly controls the manufacture of chemicals, e.g.:

- Process control computers
  - Distributed control systems
  - Programmable logic controllers
  - PCs
- Purchased equipment containing computers

Pneumatic and electromechanical control is excluded

Other Physical Systems Scope

- *Physical plant equipment* used in the manufacturing process, e.g.:
  - Raw material handling systems
  - Equipment monitoring systems
  - Waste treatment systems
- *Physical equipment* necessary to ensure uninterrupted operation of the plant, e.g.:
  - Fire detection and suppression systems
  - Perimeter security systems
  - HVAC systems

Why the Distinction? How We Started

- Original focus was on control systems
  - Highest degree of risk
  - Strong central understanding
  - Central leverage with key suppliers
  - Consistent approach to critical systems needed
- Intended to let sites manage other physical equipment independently
  - Range of equipment significantly more diverse
  - Most selection and procurement was local

Physical Systems Added to Central Program

- Different sites took very different approaches to physical systems
- Some overlap between control and other physical systems became apparent
- Found that there would be benefit in central organization
  - Better communication and information sharing
  - More uniform guidelines
  - Corporate view of status and issues at each site

Site Requirements: Control Systems

- Each site is required to build a five-tier safety net:
  - Obtain vendor certification of **every** control component
  - Test **every** system - demonstrate ability to produce
  - Analyze code where critical

  - Arrange technical coverage through and beyond midnight
  - Be prepared to identify and handle upsets and to shut down safely if necessary

Site Requirements: Control Systems

- Submit inventory
- Report testing
- Describe upset handling procedure
- Report remediation requirements
- Site manager's certification that assessment is complete

Generally complete

1999 requirements

- Complete contingency plan
- Complete transition / staffing plan
- Site manager's certification of readiness

Site Requirements: Other Physical Systems

- Inventory
- Rank criticality
- Determine appropriate assessment technique(s) for critical items
  - Vendor certification
  - Testing
  - Code analysis
- Determine and implement remediation requirements
- Report all of the above
- Determine approach for less critical items

Findings: Control Systems

- **Every** failure found was predicted by the vendor
- Use of dates limited to data acquisition and reporting
- Old control systems require upgrades
- Vendors are generally cooperative
- To date, have found only one catastrophic control system failure

Findings: Other Physical Systems

- About 5-7% of physical systems require remediation
- Typically involve PC upgrades
- Have found no catastrophic failures of physical systems
- Many identified failures have straightforward workarounds
  - Manual reset of date after 1/1/00
  - Elimination of systems
  - Manual intervention
  - "Do nothing" - noncompliance is inconvenient, but acceptable

A Final Protection Layer

- Most major problems occur while a plant is running
- Shutting down operations through the millennium transition is a prudent precaution, where practical
- Many of our plants are traditionally idle at year-end, and will be for the transition
- Planned shutdown for other sites is under consideration as part of contingency planning