

1996 CONSOLIDATED AUDIT

PROCESS CONTROL

TEAM LEADER - JOHN WILLIAMS

FUNCTIONAL LEADERS - MIKE WOODS

DO A 043132
CONFIDENTIAL

Audit Form

Plant
information

Plant Chlorine I Compliance with the GPC Minimum Security Standards

Introduction

This document identifies plant:

- compliance with the GPC Minimum Security Standards
- variances with the GPC Minimum Security Standards

Document
management

The plant maintains this document in the plant library with the process control operating discipline documentation.

A copy of this document is sent to the GPC Security. GPC maintains a database of all plant variances to the GPC Minimum Security Standards.

Audit
information

The following general audit information is required:

Audit Date:	Plant Site:
Process Information: <u>LACLW1 14.728</u> <u>LACLW2 14.664</u>	Node: <u>LACLV2</u> Plant Name: & Section _____ DEC Node: <u>14.878</u> Sys. Mgr.: Phone #: <u>6717</u> EMail Addr.: _____
Process Control Types:	Dow MOD's: <u>Yes</u> Dow OS: <u>No</u> PLC's: <u>Yes</u> Other Types <u>TDC-2000</u>
Process Information Types: <u>LACLW1 2.4</u> <u>LACLW2 2.4</u>	Dow GPI Ver.: <u>2.4</u> Dow OS Ver.: <u>No</u> Other: _____

continued on next page

DO A 043133
CONFIDENTIAL

Audit Form, continued

Minimum
requirements

The following are minimum requirements of the GPC Security Standards:

Security Minimum Requirement	Plant in Compliance (y/n/na)	Plant Variance Required & Submitted (y/n/na)	Variance Category
All devices doing Direct Process Write are within the Direct Control environment.	<u>Yes</u>		A
All Validated Data Write generated by automatic devices must be authorized, including verification of transmission and validation of range of value.	<u>Yes</u>		B1
Users performing Validate Data Write must be within the plant.	<u>Yes</u>		B2
Alarm Acknowledge only occurs within the operating area of the plant.	<u>Yes</u>		B3
MOD 5 communications between control rooms in different plants must use approved secure means: • Network controller cards • Dedicated (Ethernet) systems for MOD Servers, MODECS, and dedicated wire CISS boxes	<u>Yes</u>		C1
Inter plant communications require approval from both superintendents, or their designees.	<u>Yes</u>		C2
All programs are written (edited) in an integrated environment with version control, change control and syntax checking (like DSS in the MOD systems).	<u>Yes</u>		D1
All critical Safety and Environmental programs are simulated after they are written or altered before loading into a process control system which is running the process.	<u>Yes</u>		D2
Control System program loads are only made by personnel authorized by the superintendent, or his designee.	<u>Yes</u>		D3
Control System program loads can only be enabled in the direct control area at the time of loading.	<u>Yes</u>		D4

continued on next page

DO A 043134
CONFIDENTIAL

Audit Form, continued

Minimum requirements (continued)

Security Minimum Requirement	Plant in Compliance (y/n/na)	Plant Variance Required and Submitted (y/n/na)	Variance Category
Control System program loads are only made at times authorized by operations.	<u>Yes</u>		D5
Changes to Process Control Source Code are only made by personnel authorized by the superintendent, or his designee.	<u>Yes</u>		D6
The appropriate process control equipment is installed to work with abort programming.	<u>Yes</u>		E1
The superintendent, or his designee authorize changes to the critical process abort program.	<u>Yes</u>		E2
Access to the critical process abort program source code is independent from access to the process control programming.	<u>Yes</u>		E3
Critical Safety and Environmental abort program code is programmed by a different individual (using independent logic) than the individual coding the associated process control program. (The use of an accepted abort template such as an MCAPP template qualifies as programmed by a different individual.)	<u>Yes</u>		E4
Machine Language changes (micro's) to a running plant program are authorized by superintendent, or his designee.	<u>N/A</u>		F1
Machine Language changes (micro's) to a running plant program are only made in the direct control environment.	<u>N/A</u>		F2
The use of Remote Data Entry panels is authorized by superintendent, or his designee.	<u>N.A.</u>		G1
Remote Data Entry panels are only used within visual contact of appropriate process status data.	<u>N/A</u>		G2
<u>N/A</u>			G3

continued on next page

DO A 043135
CONFIDENTIAL