



**Process Control Systems
Industry Conference**

24x7 Managed Cyber Security for a Process Control Network

**Clayton L. Coleman, CISSP
Senior Consultant, Cyber Security
Invensys Process Systems**

**Simon Clifford
Senior Consultant
Integralis**

Agenda

- ◆ **Introductions**
- ◆ **About Husky Energy's Lloydminster Site**
- ◆ **The need for 24x7 managed services**
- ◆ **Value statements from Don Gilmour, Husky Energy**
- ◆ **Background on Managed Services from Integralis**

About the Husky Energy Lloydminster Site



- Lloydminster, Alberta
- 155 miles East of Edmonton, Alberta
- Winter average temperature:
(-13C/8F) to (-25C with wind chill)



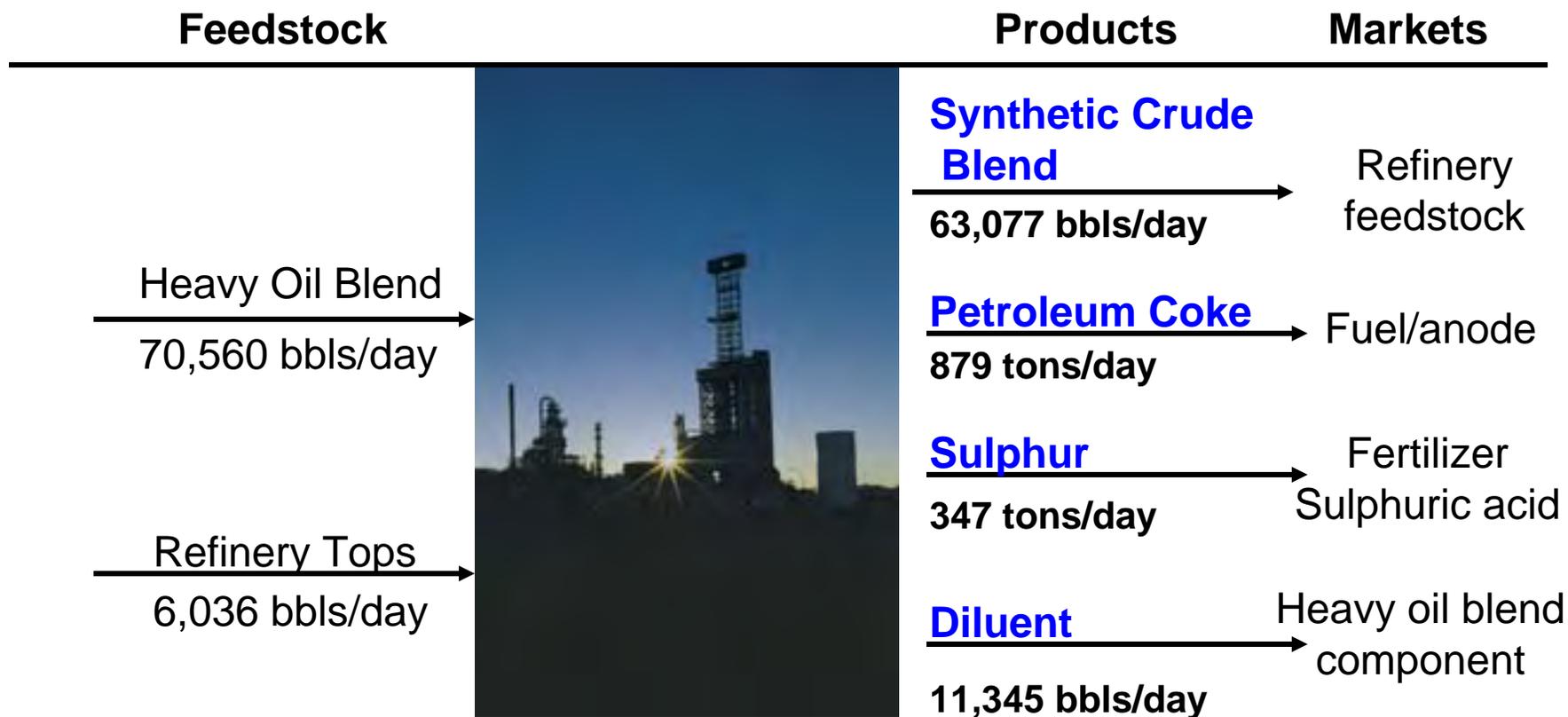
Husky Energy

IPS

INVENSYS PROCESS SYSTEMS



Lloydminster Upgrader Process Summary



Lloydminster Upgrader Fast Facts

- ◆ The Upgrader was commissioned in 1992 at an original design capacity of 46,000 barrels of synthetic crude oil per day.
- ◆ It took four years to construct the Upgrader, at a cost of \$1.6 billion.
- ◆ At peak construction, in October 1991, more than 3,800 workers were on site.
- ◆ More than 3.2 million person-hours of engineering work were invested in the project.

The Husky Cyber Security Story

- ◆ Husky process control staff knew they needed to beef up their security, but didn't know where to begin.
- ◆ Husky looked to leverage their existing on-going relationship with Invensys by seeking out expertise from Invensys' Global Consulting organization.
- ◆ Husky knew that implementing a security infrastructure meant more than a one-time activity, it would require ongoing "care and feeding."

Teaming for Success

Why did you feel the need to have an external Security Audit performed on your plant?

“With the ever changing field of cyber security management it is very difficult to stay on top of the technology while managing other areas of responsibilities. The external audit was completed by technical people, very knowledgeable and skilled in this field where there only job is cyber security. They were able to find issues which we may not have even thought of.” - Don Gilmour

Teaming for Success

Once you had the audit, were you surprised at the results. Did something really shock you?

“I was not surprised with the results found on the control network side; however I was surprised with what was found on the business network. The ease of access to the control network from the business network was just unacceptable as demonstrated during the audit.”

Don Gilmour

Teaming for Success

What did you feel you needed to do first generally?

Had you considered policies and procedures or just firewalls..etc..

“What we needed first was an idea of what a security project would entail and the paths required to implement a security system that was approved by the DCS vendor. During the audit phase it became apparent that a security system would include more than just Firewalls.”

-Don Gilmour

Teaming for Success

Did you have good corporate IT support on your plant network? Can they assist in your security posture?

“Well we had an IT group capable of assisting with this project, it was decided to use Invensys and Integralis for support for they are more familiar with control system networks and are aware of the different procedures that are required with regards to such networks.”

- Don Gilmour

Teaming for Success

How did you decide on implementing firewalls even though your plant was firewalled from the biz network?

“We had to have a definite division between the Business Network and the Control Network. The IT group was not about to let us have control over the rules in the IT firewall and the rules they did have might cause problems within the control network. By implementing the firewall on the control network side the IT group could control the traffic on their network and we can control the traffic on our network.”

- Don Gilmour

Teaming for Success

You decided to allow another company manage your security devices. What was the criteria used to determine this was right for Husky Energy?

“With the many tasks that are required of us, it is very difficult for us to monitor and manage the security devices constantly and we are not on site 24 hours a day. By having a third party manage the devices, threats and problems will be handled immediately no matter what time of the day. As well they are on top of the latest threats and they can keep the security hardware and software updated.”

- Don Gilmour

The Solution

- ◆ Needs Assessment
- ◆ Policy and Network Design
- ◆ Multi-zone DMZ Architecture
- ◆ Proxy/Relay Zone for External Communications
- ◆ Network-based Intrusion Prevention System
- ◆ Ready-to-be-managed Solution

About Integralis

- ◆ **Global Security Services Company**

- Operations in 9 countries, 21 offices, over 500 staff
- Over 250 certified technical personnel
- Over \$260M in revenue for FY2007
- Public company on the German Exchange (Symbol: AAGN)

- ◆ **Over \$40M invested in the ISIS Infrastructure**

- Follow the Sun Security Operations Centers (SOCs)
- Multilingual Technical support
- Supporting 200+ customers in 40 countries

- ◆ **Solutions focused (best solution for client)**

- ◆ **Technology platform agnostic**

Integralis - Global Footprint



▲ INTEGRALIS OFFICES

● INTEGRALIS SOC'S (Security Operations Centres)

UK	London Edinburgh Reading Warrington	USA	Los Angeles, CA Hartford, CT New York, NY Overland Pk., KS
Germany	Munich Cologne Heilbronn Hamburg Cologne	UAE	Dubai
AUSTRIA	Vienna	SWITZERLAND	Glattbrugg
		FRANCE	Givisiez
		SWEDEN	Paris
			Stockholm
			Gothenburg
		ASIA	Singapore

USA	Los Angeles, CA Hartford, CT
UK	Reading
FRANCE	Paris
GERMANY	Munich
SWEDEN	Stockholm
UAE	Dubai
ASIA	Singapore

Delivery Architecture

ISIS – comprises of:

- SSA, Datagrid, GUI and Portal

What is the SSA Appliance?

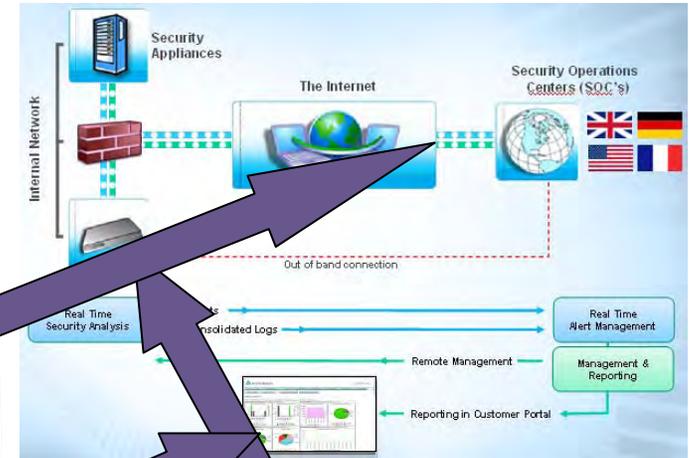
- Point of presence to customer site



MSSPortal



- Minimal bandwidth requirements
- General Status & Availability, Risk, Version
- Realtime Analysis
- Network Checks
- Remote Management Equipment – OOB Access, Console Access, Power Control



- > Full cross, multi-factor authentication
- > Attack profile Dashboard of attacks, attacked ports, new attacking IPs, Attack Management Reports
- > Real Time Alert Management (Management/mem) / Availability (SSA facing/Internet)
- > SecureEmail / Postini reporting
- > Geographical reporting
- > Ticket Management, Change Requests
- > Traffic Stats, Alert Reports, IDS Trends
- > Knowledge Base Authentication
- > Customisable Reporting Scheduler, emailer
- > Many more....

Integralis - Events / Alerts / Incidents

- Security devices generate **Events**
- SSA generates **Alerts** using defined criteria from events
- SSA applies rules, aggregation, correlation, normalisation and sends **Alerts** to ISIS via the Receivers (ISIS Datagrid)
- **Aggregation – “Many into one”**
 - Combine many identical events into a single event and set the count equal to the total
- **Normalisation – “Make common format”**
 - Convert the different log formats (syslog, SNMP Trap) into a common format
- **Correlation – “Identify patterns of events”**
 - Examine the events and look for patterns which might indicate what has occurred.
- Eg. A server reboot results in many EVENTS which can be correlated into one single ALERT called 'DEVICE REOOTED'
- Duplicates removed, Business Logic (Rules) process applied and incidents created
 - If alert is IDP/Code_red then create an incident
 - If alert is IDP/Code_red AND the destination is on the internal network then create an incident with high severity
 - If alert is IDP/Code_red AND the destination is on the internal network AND Action is Drop, then display in the portal
- Business rules can be as simple or complex as required, if data is available anything can be coded
- **Incidents** created (ISIS)
- SOC Engineers visibility through ISIS GUI and review/action incidents
- Security **Incidents** also appear in the ISIS Customer Portal

Typically thousands of events are reduced to hundreds of Alerts and in turn create a few Incidents



Husky Managed Security Services Value-Add

◆ Co-Managed Service offering

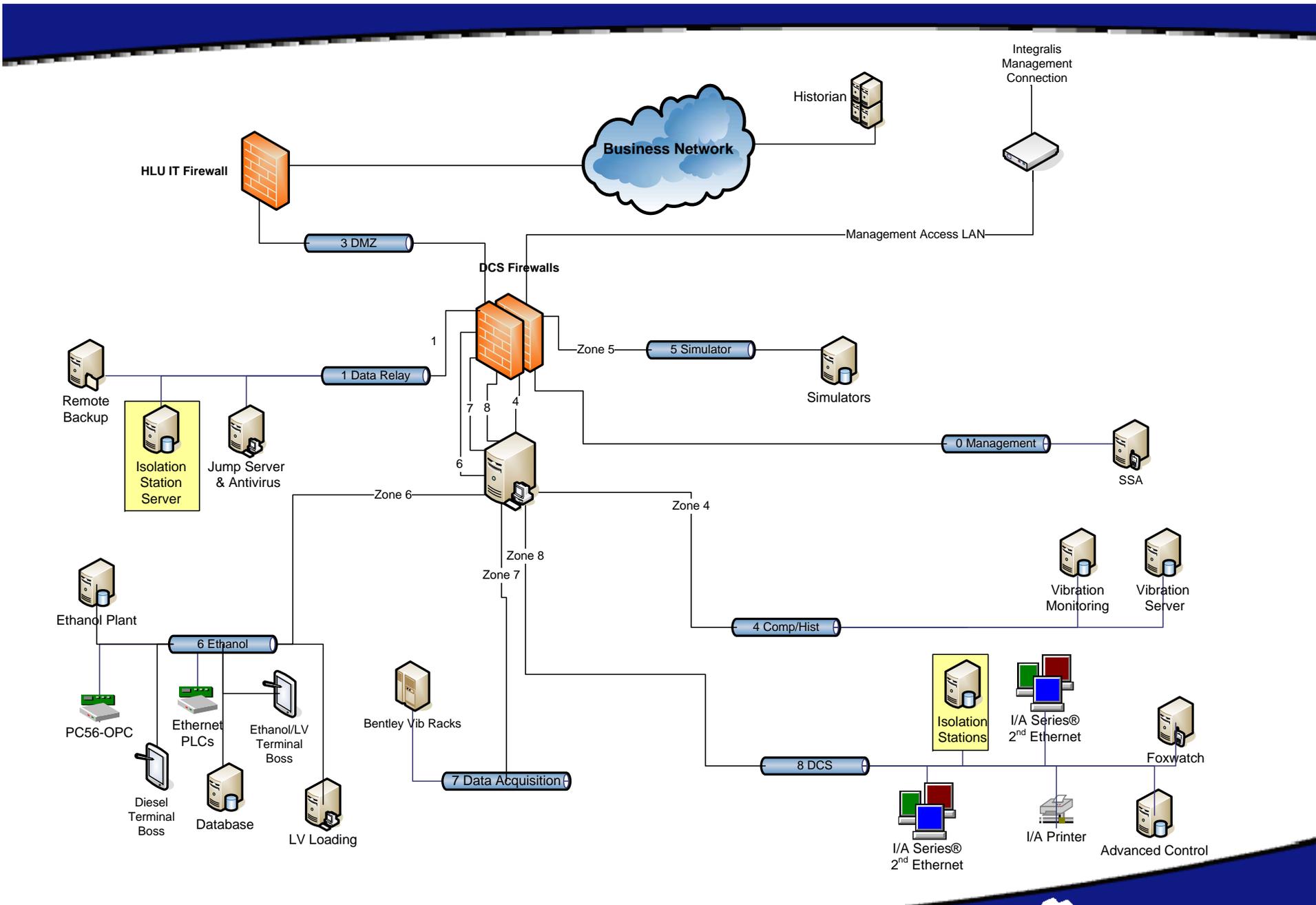
- Husky retains control
- Leverages Integralis Security Expertise & 24 x 7 Operations
 - Patches reviewed, Husky notified for approval, then applied
 - Signature and Rule changes, Attack Updates applied
 - Less vulnerable

◆ Initial Deployment

- SSA device deployed, connectivity devices and SOC tested
- Escalation procedures defined & tested
- Security policy & business rules set-up and tuned for Husky over 2 month period
- Secure Portal - reporting and dashboards tuned

◆ Since deployment

- 24 x 7 monitoring & management of Husky infrastructure
- Multiple patches, signature, and rules changes assessed and applied
- No outages!



Husky Security Service Delivery Components

- **7 x 24 Service Availability**
- **SSA (Security Service Appliance) Device**
- **Remote Management Equipment (Power cycling)**
- **System Availability Checks**
 - Critical processes running, System availability, Uptime/Reboots
- **Extended Availability Monitoring**
 - DNS / FTP / SNMP / Radius server checks, HTTP & HTTPS page Checks, ICMP Ping check, SMTP protocol, TCP open port check
- **System Health Monitoring**
 - CPU usage, Disk/Flash Space, Memory/Swap Space, Version (HW, OS, FW, SSH)
- **System Health Alerting & Escalation**
- **System Configuration Backup**
- **Secure Portal Access**
- **Reporting**
 - System availability & health, Administrative - tickets, change requests, Service Delivery - Alerts, Incidents, Traffic, policy change, system access
- **Vulnerability Monitoring**
- **Rulebase / Policy Management**
- **Full Logfile Analysis (Security Event Monitoring)**
 - Management server process, policy, configuration, anti-spoofing, DOS, Alerts correlated, Hostport Scans, system access
 - Device process status, configuration changes, system access, Alerts correlated by source/destination, sensor statistics
- **Security Alerting and Escalation**
- **Remote System rebuilds**
 - Within two hours of hardware replacement
- **Platform management**
- **Service Level agreement – response times, escalation...**

Final Message from Don

“We take our security program very seriously and it is very high on our priority list.”

Don Gilmour

Contacts

Clayton L. Coleman

Invensys Process Systems

clayton.coleman@ips.invensys.com

Don Gilmour

Husky Energy

don.gilmour@huskyenergy.ca

Simon Clifford

Integralis

simon.clifford@integralis.com