

Kevin Staggs, CISSP  
June 7, 2006

# Security Metrics

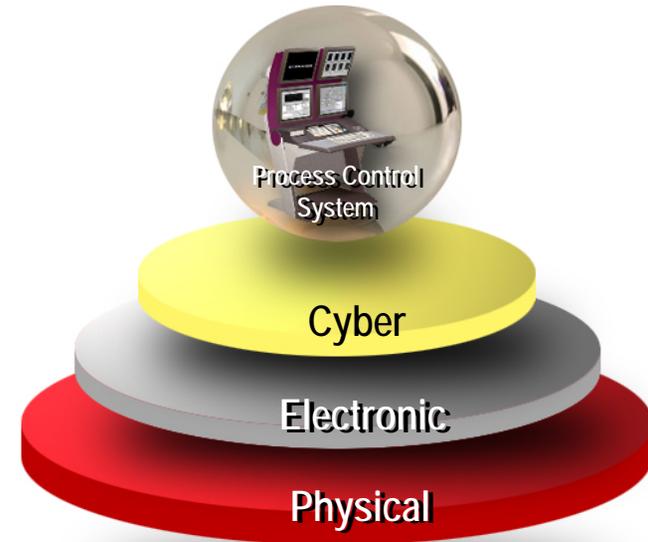
**Honeywell**

## Topics

- Our Philosophy
- Metrics at our Chemical Plants
- Metrics for Product Development

# Our Philosophy

- Security and safety
  - Without security you cannot have safety
- Key Honeywell initiative
- Defense in depth
  - Security at more than just the perimeter
  - Built-in at every layer of the system
- Security is a journey not a destination
  - Policies and practices are key
  - Continuous security testing and improvements



# Metrics at our Chemical Plants

- Evaluation based on Industrial Security Specification
  - Created by Honeywell Process Solutions
    - Made available on request
  - Includes:
    - Physical security
    - Cyber security
    - Process control specific areas
- All Tier 1 and Tier 2 sites evaluated
  - 9 total sites
  - Stoplight ratings for each site
- Prioritized investments based on evaluation

## Metrics at our Chemical Plants

<b>Cyber</b>	H	Process Control Cyber Security Team	Yellow								
	H	Process Control Cyber Security Team Responsibilities	Green								
	H	Process and Practices related topic	Red								
	H	Physical Security of Computers	Red	Green	Red	Red	Yellow	Green	Yellow	Blue	Red
	H	Physically layered topology	Yellow	Yellow	Yellow	Yellow	Green	Yellow	Green	Blue	Yellow
	H	Process control network security	Green	Green	Green	Green	Green	Green	Blue	Green	Green
	H	Process control network environmental	Green	Green	Green	Green	Green	Yellow	Blue	Green	Green
	H	Remote access	Yellow								
	H	Anti virus software	Yellow	Yellow	Yellow	Yellow	Blue	Yellow	Green	Blue	Yellow
	H	Security hotfix deployment	Green	Yellow	Yellow	Green	Green	Green	Yellow	Blue	Red
	H	Process control system security	Green	Green	Green	Green	Green	Green	Blue	Green	Green
	M	Backup and recovery	Green	Green	Red	Green	Green	Green	Yellow	Blue	Green

## Development Metrics

- Utilize Six-Sigma FMEA tooling
- FMEA output used to justify development activities
  - Control Firewall justification example

ID #	Process Step/Input	Potential Failure Mode	Potential Failure Effects	SEV	Supporting SEV reasons	Potential Causes	OCC	Supporting OCC reasons	Current Controls	DET	RPN	Actions Recommended	
	A sequential number to allow column sorting to restore sheet to original appearance.	What is the process step / item function under investigation?	In what way could the process step/function potentially fail to meet process requirements or intent?	What is the impact on the Key Output Variables (Customer Requirements) or internal requirements?	How Severe is the effect to the customer?		What are the causes of this Failure Mode? Typical causes result from process input failures (review Process Map).	How often does cause of FM occur?		What are the existing controls and procedures (inspection and test) that prevent the cause or the Failure Mode?	How well can you detect cause of FM?	SEV * OCC * DET	What are the actions for reducing the occurrence of the Cause, or improving detection? <b>Should have actions only on high RPN's or easy fixes.</b>
1	receiver node/port	broadcast storm	Dimished BW at other receivers (causes other msgs to be blocked)	3	ports are RR?	malicious software	1	hacker must be onsite	Broadcom parts do broadcast storm control	2	6	Better use of Broadcast storm protection on Broadcom part, use security features of 2950	
2	receiver node/port	broadcast storm	Dimished BW at other receivers (causes other msgs to be blocked)	3		manual error	3		Broadcom parts do broadcast storm control	2	18	Better use of Broadcast storm protection on Broadcom part	
3	receiver node/port	broadcast storm	Dimished BW at other receivers (causes other msgs to be blocked)	3	ports are RR?	defective software outside cabinets	3		Broadcom parts do broadcast storm control	5	45	use 2950 storm mitigation on outgoing ports (maybe MII anti jabber) Enable broadcast/multicast limiting on 9 port switch	

1 = No likelihood that L1 control ceases  
 3 = Very little likelihood that L1 control ceases  
 5 = Some likelihood that L1 control ceases

\* KASOM = Knowledge and Skills of Manpower

0 = Can't occur  
 1 = Occurs every 20 years  
 3 = Occurs every 5 years  
 5 = Occurs every year  
 7 = Occurs monthly over one customer's sites

0 = inherently prevents/overcomes  
 1 = Easy to prevent/discover  
 3 = Hard to prevent/discover  
 5 = Very hard to prevent/discover given current controls

## Summary

- Chemical Plant Security
  - Metrics prioritize security investment
    - Physical
    - Cyber
    - Policies and practices
- Product Development
  - Six Sigma FMEA used to prioritize security developments