Threat Identification and Response

PHMSA R&D Forum

Chad Zamarin, Colonial Pipeline Company

February 7-8, 2007

Threat Identification

Ideal Attributes

☑ All threats to a system are considered

☑ As conditions change, threat identification updates

☑ Multiple threat interaction is understood and accounted for

☑ When threats are identified, appropriate response is efficiently planned

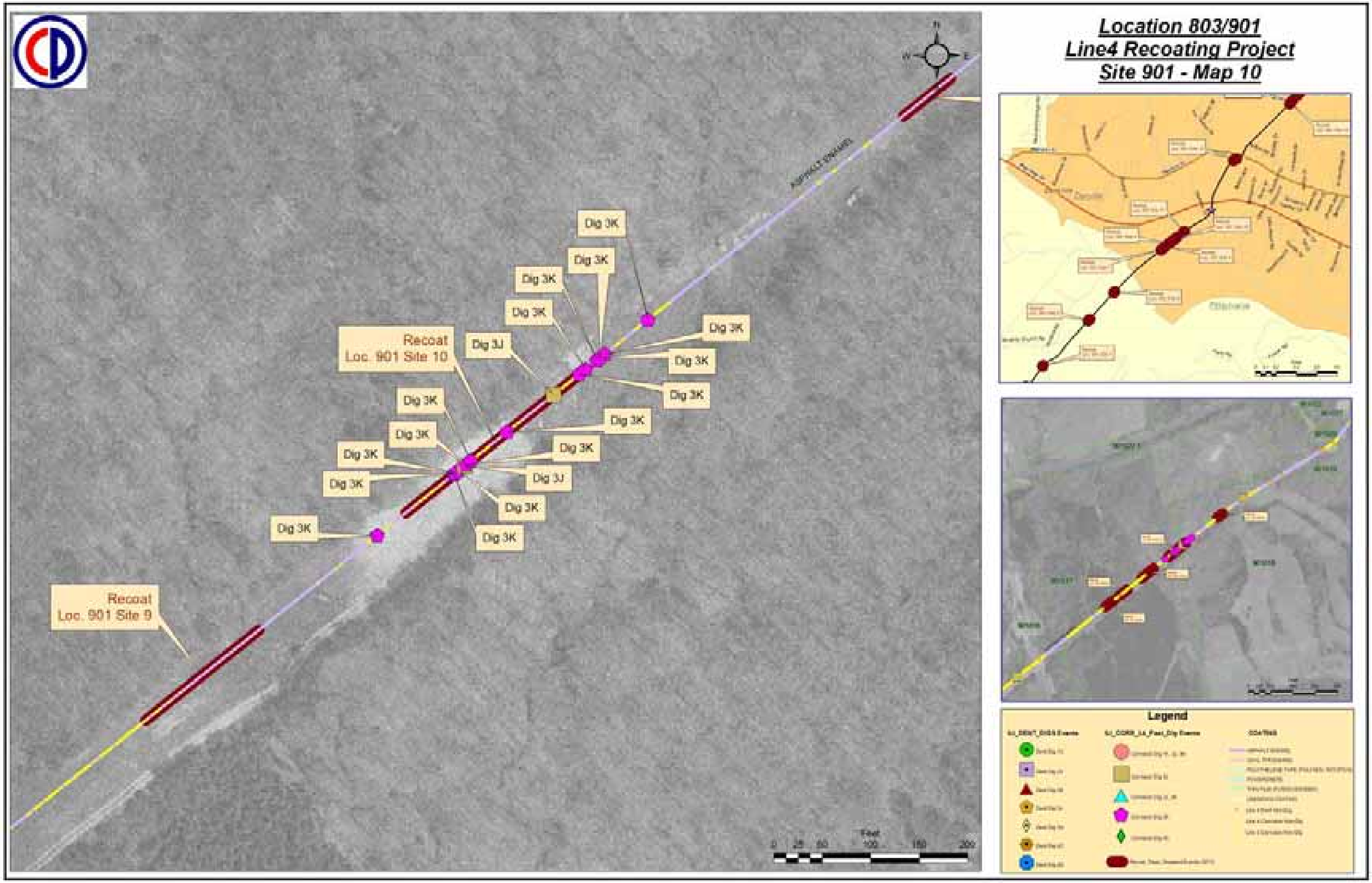
☑ Responses are targeted to the threat or combination of threats

☑ Response and mitigation information is immediately fed back to the threat Identification system to validate predictions or update assumptions.

☑ Threats are properly prioritized, effectively communicated and performance is easily measured.

☑ The system relies on integrated data from all sources in real time (SCADA, inspection data, One call activity, weather, etc.)

Threat Identification



Threat Identification

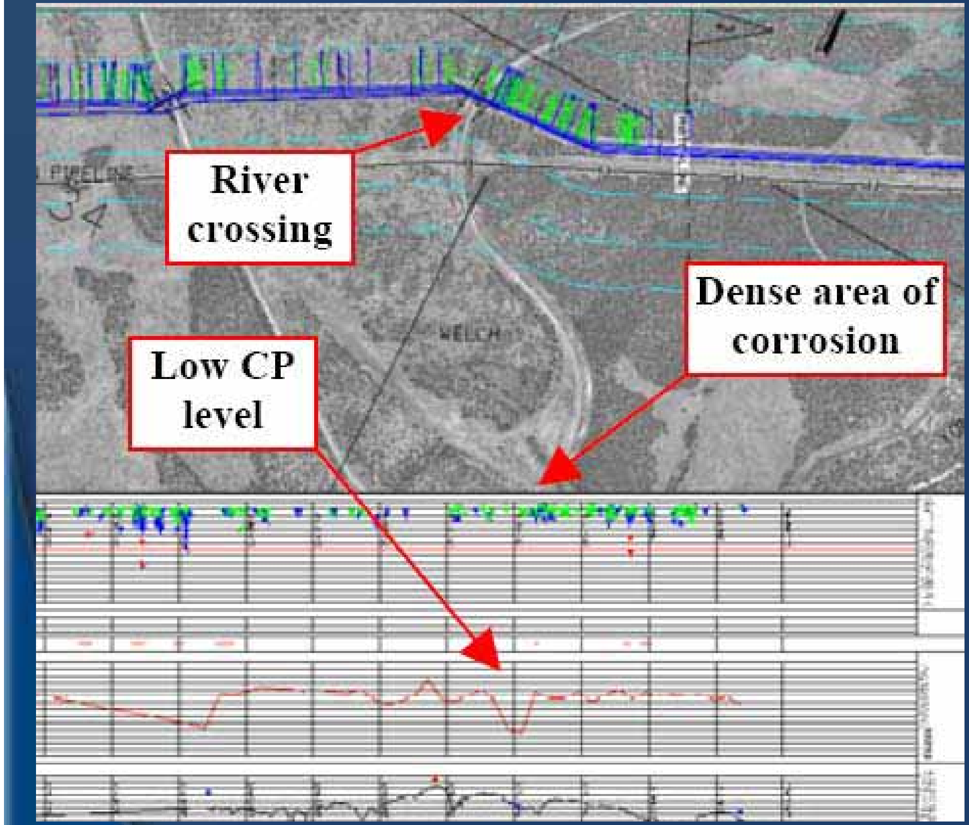
Ideal Attributes

☑ The threat identification system is a “learning” system

- Less well understood threats are modeled in a basic fashion
- As data collection and information grows, models adjust based on findings
- Ongoing sensitivity testing, algorithm refinement and incorporation of learnings and developments outside te organization

☑ The threat identification system performs efficient systemic analysis to model similar locations

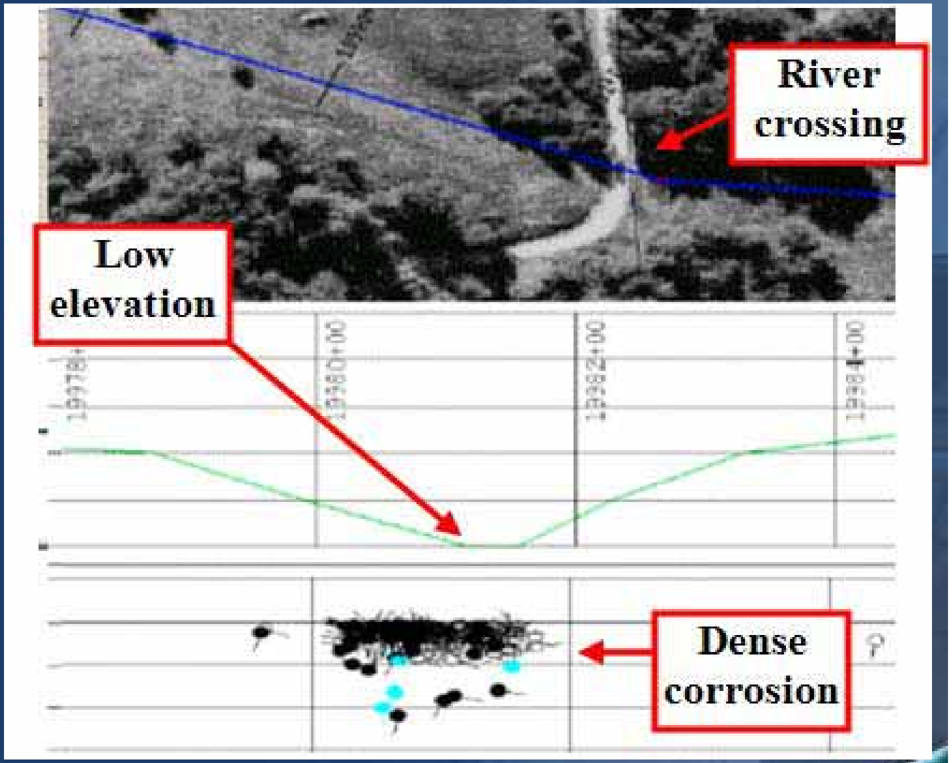
Threat Identification



River crossing

Dense area of corrosion

Low CP level



River crossing

Low elevation

Dense corrosion

Threat Identification

Ideal Attributes

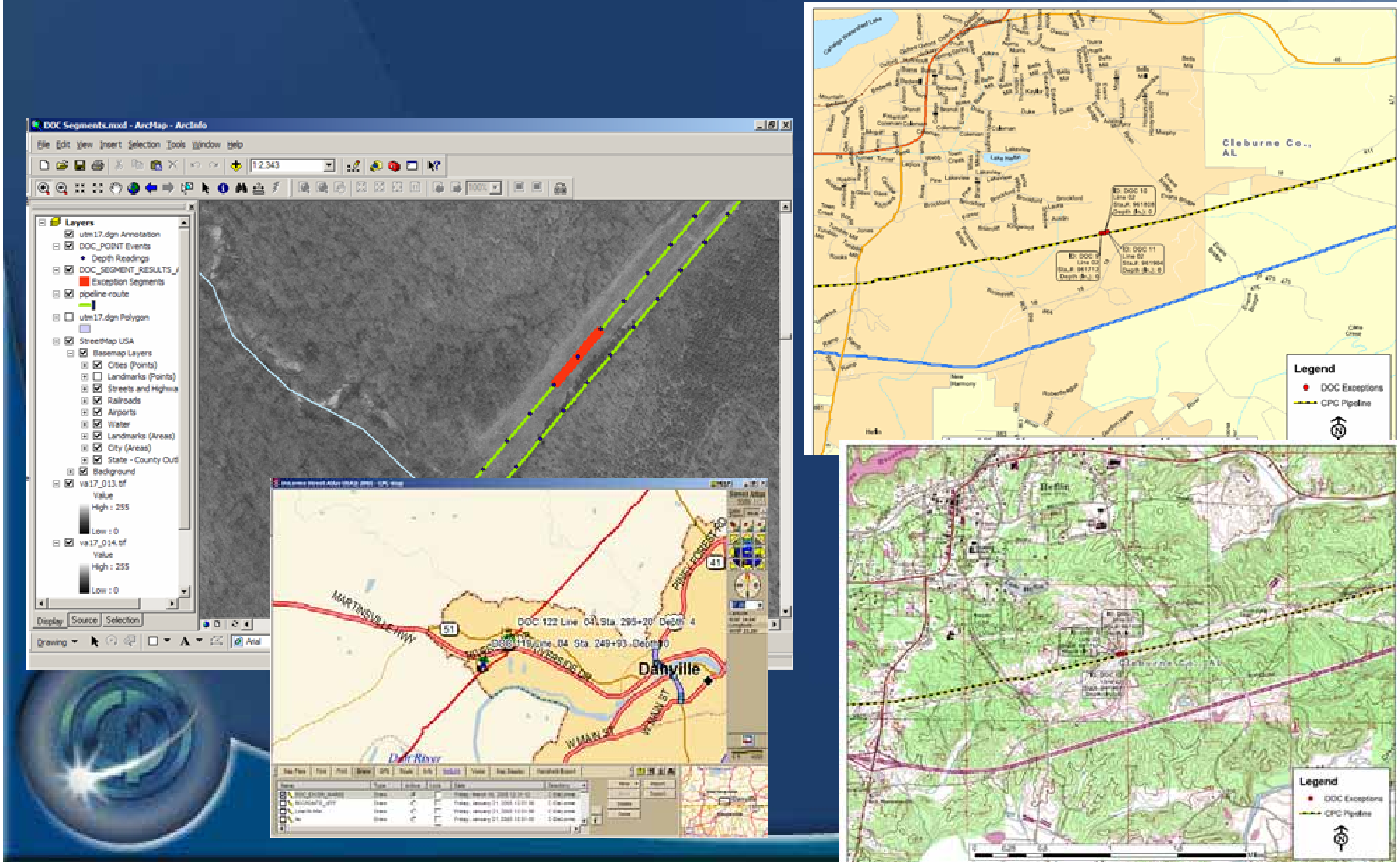
☑ Threat identification occurs at multiple levels

- System wide – relative and probabilistic = program planning
- Focused – probabilistic and quantitative = project planning

☑ Outputs are readily available at multiple levels

- Analytical – SME use for threat monitor and system improvement
- Visual – for use by broader audience to validate, plan, analyze and make decisions
- Dashboard – to measure performance (the heartbeat of the organization)
- Broad distribution of threat and risk assessment is critical.

Threat Identification



Threat Identification

Common Issues

☑ Good data needed to feed analysis is often not readily available in an integrated, ready to use format

☑ Response selection is not inherently tied to threat identification

☑ Data feedback is slow or sometimes not occurring

☑ Data management overhead limits time for analysis and response.

☑ Far from real time

☑ Heavily dependent on SME’s turning the crank and using the results

☑ Limited distribution of threat and risk systems, limiting value

Threat Identification

Common Issues

☑ Models are static, slow to improve

☑ Too often there is a focus on risk management bells and whistles over content and application (form over substance)

☑ Focus has been heavily on models and less on tools to make risk management more integral to operations (communication, integration, planning, evolution, etc.)

☑ Systems are often myopic - Program level prioritization, or trying to pinpoint the next failure, etc.

Gaps

- ☑ Underlying integration technologies – how do we make integration inherent?
- ☑ Lack of risk management consensus minimum standards across liquid and gas
- ☑ Technology to provide learning systems
- ☑ Bandwidth to get real time feedback
- ☑ Dynamic system to measure real time threats and changes
- ☑ High resolution threat analysis with roll up capabilities
- ☑ Spatial analysis

Opportunities

?