



S-MAP Workshop 1

- | | | |
|------------------------|---|---|
| Jorge DaSilva | – | <i>Director, Operations Risk Management</i> |
| David Cheng | – | <i>Operations Risk Manager</i> |
| Scott King | – | <i>Director, Information Security</i> |
| Mari Shironishi | – | <i>Pipeline Integrity Risk & Threat Team Lead</i> |
| Mason Withers | – | <i>Quantitative Risk and Controls Manager</i> |
| Greg Flores | – | <i>Director, Enterprise Risk Management</i> |

August 3, 2015



Introduction – Key Messages

- The S-MAP outcome will determine whether or not the presented models can be used as the basis for each energy utilities' RAMP filing in its respective GRC.
- SoCalGas and SDG&E's processes and tools presented today will enable the two companies to complete their November 2016 RAMP filings.
- The level of sophistication of risk assessment methodologies is directly proportional to the magnitude of the risk for which it is conducted.
- SoCalGas and SDG&E's processes for identifying and evaluating risk follow the methods adopted in International Organization for Standards ("ISO 31000") and the approaches proposed by Cycla in Pacific Gas and Electric Company's 2014 GRC.
- SoCalGas and SDG&E's risk management processes are evolving and will continue to evolve.
- The implementation of SoCalGas and SDG&E's risk management processes will follow a similar trajectory as the evolution and creation of SDG&E's exemplary safety culture.



Introduction - Vision

Vision

SoCalGas and SDG&E's risk management vision is to implement leading practices that promote transparency and integrate enterprise and operational asset risks into investment decisions to minimize stakeholders' exposure to safety, security and reliability risks.

Potential actions we anticipate to take to achieve the vision:

- Develop qualitative (near term) and quantitative (long term) methods for risk evaluation and measurement.
- Demonstrate transparent, repeatable and consistent decision making risk management processes that result in cost effective risk mitigation.
- Incorporate subject matter expertise that has been calibrated into our risk analyses and management and validate it by collecting supporting data.
- Introduce processes and procedures that seamlessly integrate asset life cycle analysis into risk management and investment management processes
- Introduce measurable and auditable metrics that demonstrate the effectiveness of risk management.
- Understand risk tolerance levels that support corporate objectives and stakeholder values.
- Establish a method for comparing alternatives for risk mitigation.



Risk Management Process

Cycla Model	Corresponding Step in SoCalGas and SDG&E's Risk Management Process
1. Identify Threats	1. Risk Identification
2. Characterize Sources of Risk 3. Identify Candidate Risk Control Measures (RCMs)	2. Risk Analysis
4. Evaluate the Anticipated Risk Reduction for Identified RCMs	3. Risk Evaluation
5. Determine Resource Requirements for Identified RCMs 6. Select RCMs Considering Resource Requirements and Anticipated Risk Reduction	4. Risk Mitigation Plan Development and Documentation
7. Determine Total Resource Requirement for Selected RCMs 8. Adjust the Set of RCMs to be Presented in GRC Considering Resource Constraints 9. Adjust RCMs for Implementation following CPUC Decision on Allowed Resources	5. Risk-Informed Investment Decisions and Risk Mitigation Implementation
10. Monitor the Effectiveness of RCMs	6. Monitoring and Review



Introduction - Agenda

Risk Evaluation Framework

Cybersecurity

TIMP

FiRM

Annual Planning Process

- **Risk Evaluation Framework – David Cheng**
 - ERM Risk Evaluation Framework, Illustrative Example
- **Cybersecurity Risk Management – Scott King**
 - Context, Process, Tool, Illustrative Example
- **Transmission Integrity Management (TIMP) – Mari Shironishi**
 - Context, Process, Tool, Illustrative Example
- **Fire Risk Management (FiRM) – Mason Withers**
 - Context, Process, Tool, Illustrative Example
- **Annual Planning Process – Greg Flores**



Risk Evaluation Framework

Cybersecurity

TIMP

FiRM

Annual Planning Process

RISK EVALUATION FRAMEWORK

DAVID CHENG – OPERATIONS RISK MANAGER



Revised Risk Score Algorithm

Risk Evaluation Framework

Cybersecurity

TIMP

FiRM

Annual Planning Process

- Revised risk score algorithm:

$$\text{Risk score} = \sum_{i=1}^n \text{weight}_i * \text{frequency}_i * 10^{\text{impact}_i}$$

Current weight values:

i	Category	Weight
1	Safety	40%
2	Reliability	20%
3	Compliance	20%
4	Financial	20%

Frequency values:

Frequency rating	Value (annual)
1	0.005
2	0.018
3	0.058
4	0.183
5	0.577
6	3.162
7	31.623

Example: Per 7x7 matrix, frequency of 4 is once every 3-10 years. Value of 0.183 represents approximately once every 5.5 years.



7x7 Risk Evaluation Matrix

Risk Evaluation Framework

Cybersecurity

TIMP

FiRM

Annual Planning Process

	Impact						
	7	6	5	4	3	2	1
	Catastrophic	Severe	Extensive	Major	Moderate	Minor	Insignificant
Health, Safety, & Environmental: Endanger workplace or public safety; impact to surrounding environment; Long-term: 10+ years Medium-term: 3-10 years Short-term: 1-3 years	Multiple fatalities or life threatening injuries; Immediate, severe, and irreversible impacts to environment	Fatality or life threatening injury; Severe and long-term impacts to environment	Many serious injuries to employees or the public; Significant and medium-term impacts to environment	Severely harm a few employees or the public; Significant and short-term impacts to environment	Result in OSHA reportable event; Moderate and short-term impacts to environment	Result in OSHA reportable event; environmental impact is immediately correctable or contained within small area	Result in OSHA reportable event; no environmental impact
Operational and Reliability: Disruption to company operations that could impact customers; may be measured in quantity of impacted customers, critical locations, loss of energy flows, and/or duration	> 1 MM customers affected; or impacts an entire metropolitan area, including critical customers; or disruption of service of more than a year due to permanent loss to a facility	>100 K customers affected; or impacts multiple critical locations and customers; substantial disruption of service greater than 1 months	> 50 K customers affected; or impacts multiple critical locations or customers; substantial disruption of service greater than 10 days	> 10 K customers affected; impacts single critical location or customer; disruption of service greater than 1 day	> 1 K customers affected; impacts single critical location or customer; disruption of service for 1 day	> 100 customers affected; impacts small area with no disruption to critical location or customer; disruption of service less than 1 day	< 100 customers affected; impacts small localized area with no disruption to critical location/customer; disruption of service less than 3 hours
Regulatory, Legal, & Compliance: Diminishing relationship and increased scrutiny by regulators or government agencies; ongoing media coverage forces outreach to policy makers/regulators; increasing stakeholder revolt or objections leading to increased oversight; loss of license, exclusivity, or monopoly	Actions resulting in closure, split, sale of the company, or criminal conviction	Cease and desist orders are delivered by regulators; Critical assets and facilities are forced by regulators to be shut down; revoking license, market-based rate authority, or monopoly	Governmental, regulatory investigation (including criminal), and enforcement actions lasting longer than one year; violations that result in fines/penalties and large non-financial sanctions	Violations that result in fines or penalties, or a regulator enforces non-financial sanctions, or significant new and updated regulations are enacted as a result of an event	Violations that result in fines or penalties	Self-reported or regulator identified violations with no fines or penalties	No impact to administrative impact only
Financial : Potential financial loss, including disallowance, legal actions or fines, replacement energy, remediation, damage to 3rd party properties, etc.	Loss > \$3 billion Ability to raise capital significantly impacted; or decrease in stock price greater than 25%; or potential insolvency	\$1 B - \$3 B Ability to raise capital is challenged; or decrease in stock price greater than 15%	\$100 MM - \$1 B Ability to raise capital becoming more difficult; or decrease in stock price greater than 5%	\$10 MM - \$100 MM	\$1 MM - \$10 MM	\$50 K - \$1 MM	< \$50 K
	Frequency/Likelihood						
	7	6	5	4	3	2	1
	Common	Regular	Frequent	Occasional	Infrequent	Rare	Remote
Frequency of an occurrence: How often does the risk event occur	> 10 times per year	1-10 times per year	Once every 1-3 years	Once every 3-10 years	Once every 10-30 years	Once every 30-100 years	Once every 100+ years



Sample Risk Score Calculation

Risk Evaluation Framework

Cybersecurity

TIMP

FiRM

Annual Planning Process

- Illustrative risk example

$$\text{Risk score} = \sum_{i=1}^n \text{weight}_i * \text{frequency}_i * 10^{\text{impact}_i}$$

Safety Impact	Reliability Impact	Compliance Impact	Financial Impact	Frequency
6	5	5	6	5

(Using frequency table, frequency 5 has value of 0.577)

$$\begin{aligned}
 &= 0.4 * 0.577 * 10^6 \text{ [safety]} + 0.2 * 0.577 * 10^5 \text{ [reliability]} \\
 &\quad + 0.2 * 0.577 * 10^5 \text{ [compliance]} + 0.2 * 0.577 * 10^6 \text{ [financial]} \\
 &= 230,800 \text{ [safety]} + 11,540 \text{ [reliability]} + 11,540 \text{ [compliance]} \\
 &\quad + 115,400 \text{ [financial]} \\
 &= \mathbf{369,280}
 \end{aligned}$$



Relative Portfolio Risk Analysis vs. More Complex Individual Risk Modeling



Risk Evaluation Framework

Cybersecurity

TIMP

FiRM

Annual Planning Process

- Risk evaluation matrix and risk score provide a uniform way of assessing risks throughout the enterprise in order to assess, prioritize, and manage the enterprise portfolio of risks
- For more complex risks, more sophisticated and detailed models are developed to enable more granular modeling and decision-making.
- Not all risks warrant a detailed risk model as it would be cost prohibitive and impractical.
- Showcase 3 examples of more complex modeling for selected risks:
 - Cybersecurity risk
 - Pipeline safety and integrity risk
 - Wildfire risk



Risk Evaluation Framework

Cybersecurity

TIMP

FiRM

Annual Planning Process

CYBERSECURITY RISK MANAGEMENT

SCOTT KING- DIRECTOR, INFORMATION SECURITY



Cybersecurity Risk Management

Risk Evaluation Framework

Cybersecurity

TIMP

FiRM

Annual Planning Process

Control Examples

Ineffective security skills training

Ineffective administrative privileges monitoring)

Ineffective malware defenses

Ineffective vulnerability analysis / mitigation

Ineffective device inventories

Ineffective data loss prevention

Initial Impact of Control Failure

Email system is compromised

Insider steals/uses information inappropriately

Undetected malware accesses sensitive information

Laptop with unencrypted sensitive information is stolen or lost

Negative Business Result: Risk Realized

Grid control is compromised

Customer information is disclosed





Cybersecurity Risk Management - Context

Risk Evaluation Framework

Cybersecurity

TIMP

FiRM

Annual Planning Process

- Cybersecurity risks defined using a recognized matrix of critical security controls
- Individual security controls are evaluated and ranked using the 7x7 model
- The Department of Energy (DOE) cybersecurity capability maturity model (C2M2) is used to evaluate cyber program maturity
- Control risks are mapped to C2M2 model
- Combined risk/maturity model used to define cybersecurity program priorities, projects, and improvements



Cybersecurity Risk Management - Tool

Risk Evaluation Framework

Cybersecurity

TIMP

FiRM

Annual Planning Process

- SANS Institute develops and maintains the critical security controls model
 - Model applicable across industry verticals
- Department of Energy publishes the cybersecurity capability maturity model
 - Three versions, electric sector, downstream natural gas, and generic
 - We use the generic version and apply to all supported companies (Sempra, SoCalGas, and SDG&E)

References:

DOE C2M2 Program - <http://energy.gov/oe/services/cybersecurity/cybersecurity-capability-maturity-model-c2m2-program>

SANS Critical Security Controls - <https://www.sans.org/critical-security-controls/>



Cybersecurity Risk Management - Illustrative Example



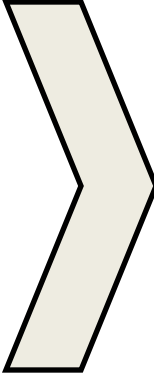
Risk Evaluation Framework

Cybersecurity

TIMP

FiRM

Annual Planning Process

SANS Controls	MAPPING	C2M2 Maturity Domain
Continuous vulnerability assessment and remediation		Threat and vulnerability management (TVM)
Red teaming and penetration testing		RATED: Medium maturity <input type="radio"/> CAUSE: Process and skillset gaps <input type="radio"/>
RATED: High risk <input checked="" type="radio"/> CAUSE: Lack of trained resources and tools <input type="radio"/>		ACTION: Investment in technology, training, and specialized resources <input type="radio"/> <input type="radio"/> <input checked="" type="radio"/>

NOTE: The above is an illustrative example only



Risk Evaluation Framework

Cybersecurity

TIMP

FiRM

Annual Planning Process

TRANSMISSION INTEGRITY MANAGEMENT PROGRAM (TIMP)

MARI SHIRONISHI- PIPELINE INTEGRITY RISK & THREAT TEAM LEAD



Transmission Integrity Management Program - Overview



Risk Evaluation Framework

Cybersecurity

TIMP

FiRM

Annual Planning Process

- Pipeline Safety Improvement Act of 2002
- 49 Code of Federal Regulations (CFR) Part 192 Subpart O Gas Transmission Pipeline Integrity Management
 - Identify the threats to pipelines in High Consequence Areas (HCAs)
 - Analyze the risk posed by these threats
 - Collect information about the physical condition of pipelines
 - Take actions to address the applicable threats and integrity concerns to increase safety and preclude pipeline failures



Transmission Integrity Management Program - Requirements



Risk Evaluation Framework

Cybersecurity

TIMP

FiRM

Annual Planning Process

- **Baseline Assessment Requirements**
 - 50% of the highest risk covered segments were required to be assessed by December 17, 2007
 - Complete assessment of all covered segments by December 17, 2012
- Prescriptive assessment interval based on assessment results, not to exceed 7 yrs



Transmission Integrity Management Program - Risk Basic Concepts



Risk Evaluation Framework

Cybersecurity

TIMP

FiRM

Annual Planning Process

Risk = Likelihood of Failure x Consequences of Failure

Likelihood of Failure (LOF) - Calculated from the sum of 9 threat groups

- External Corrosion (EC)
- Internal Corrosion (IC)
- Stress Corrosion Cracking (SCC)
- Manufacturing (M)
- Construction (C)
- Equipment (EQ)
- Third Party Damage (TPD)
- Incorrect Operations (IO)
- Weather Related and Outside Force (WROF)

Consequences of Failure (COF) - Calculated from the sum of 3 factors

- Potential Impact Radius (PIR)
- Class Location
- Stress Level



Transmission Integrity Management Program - Data Considered for LOF

Risk Evaluation Framework

Cybersecurity

TIMP

FiRM

Annual Planning Process

Threat Category	Type of Data				
	EC	Install Year	Coating Type	Cathodic Protection Criteria	
IC	Install Year	IC Threat Presence			
SCC	Install Year	Coating Type	% SMYS	20 miles D/S of Compressor Station	
M	Install Year	Coating Type	Material	Long Seam Type	Cathodic Protection Criteria
C	Install Year	Girth Weld Type	Wrinkle Bend Presence		
EQ	Install Year	EQ Failure Presence			
TPD	Install Year	Class Location	Foreign Line Crossing	Presence of Farmland	
IO	Install Year	IO Event Presence			
WROF	Install Year	Liquefaction	Slope	Landslide	Alquist Priolo Fault



Transmission Integrity Management Program - LOF Weighting Factors



Risk Evaluation Framework

Cybersecurity

TIMP

FiRM

Annual Planning Process

- The percentage weighting of 9 threats:

	Initial Targets	DOT Stats 1984-2001	DOT Stats 2002-pres	Initial Final Weights	Updated Final Weights
External Corrosion	20	14	11	20	20
Internal Corrosion	15	17	15	10	5
Stress Corrosion Cracking	6	0	0	4	1
Manufacturing	10	12	9	9	20
Construction	15	6	9	10	8
Equipment	1	1	9	2	2
Third Party Damage	22	36	28	33	37
Incorrect Operations	1	4	3	2	2
Weather Related and Outside Force	10	10	16	10	5
Totals	100	100	100	100	100

- Various LOF thresholds depending on threats
 - System wide threats for external corrosion & third party damage



Transmission Integrity Management Program - Relative Risk Score



Risk Evaluation Framework

Cybersecurity

TIMP

FiRM

Annual Planning Process

$$RRS = \frac{LOF \cdot COF}{10,000}$$

- Max LOF score of a segment is 1000
- Max COF score of a segment is 1000
- Maximum Relative Risk Score (RRS) for each dynamic segment is 100
- LOF, COF & RRS are calculated by Risk Frame Modeler (RFM)
- Max dynamic segment RRS gets assigned to the pipeline



Transmission Integrity Management Program - Example



Risk Evaluation Framework

Cybersecurity

TIMP

FiRM

Annual Planning Process



Pipeline Name	Max Risk Score	Dynamic Segment Risk Score	Dynamic Segment Length (mile)	COF				LOF
				COF Score	PIR	Class Location	% SMYS	LOF Score
A	27	27	0.1	590	230 ft	Class 3	43%	460
A	27	15	0.3	320	230 ft	Class 1	43%	460 ²³



Transmission Integrity Management Program - Risk Mitigation Planning



Risk Evaluation Framework

Cybersecurity

TIMP

FiRM

Annual Planning Process

Risk Mitigation

- Assessment method selection
 - ILI, Direct Assessment, Pressure Testing & other technologies
- Expanding assessment to non HCA
- Defect Assessments & Remaining life calculation
- Repair/replacement decisions
- Determination of assessment interval
- Further preventative actions identified
- SoCalGas and SDG&E are continually making improvements and committed to safety and compliance



Risk Evaluation Framework

Cybersecurity

TIMP

FIRM

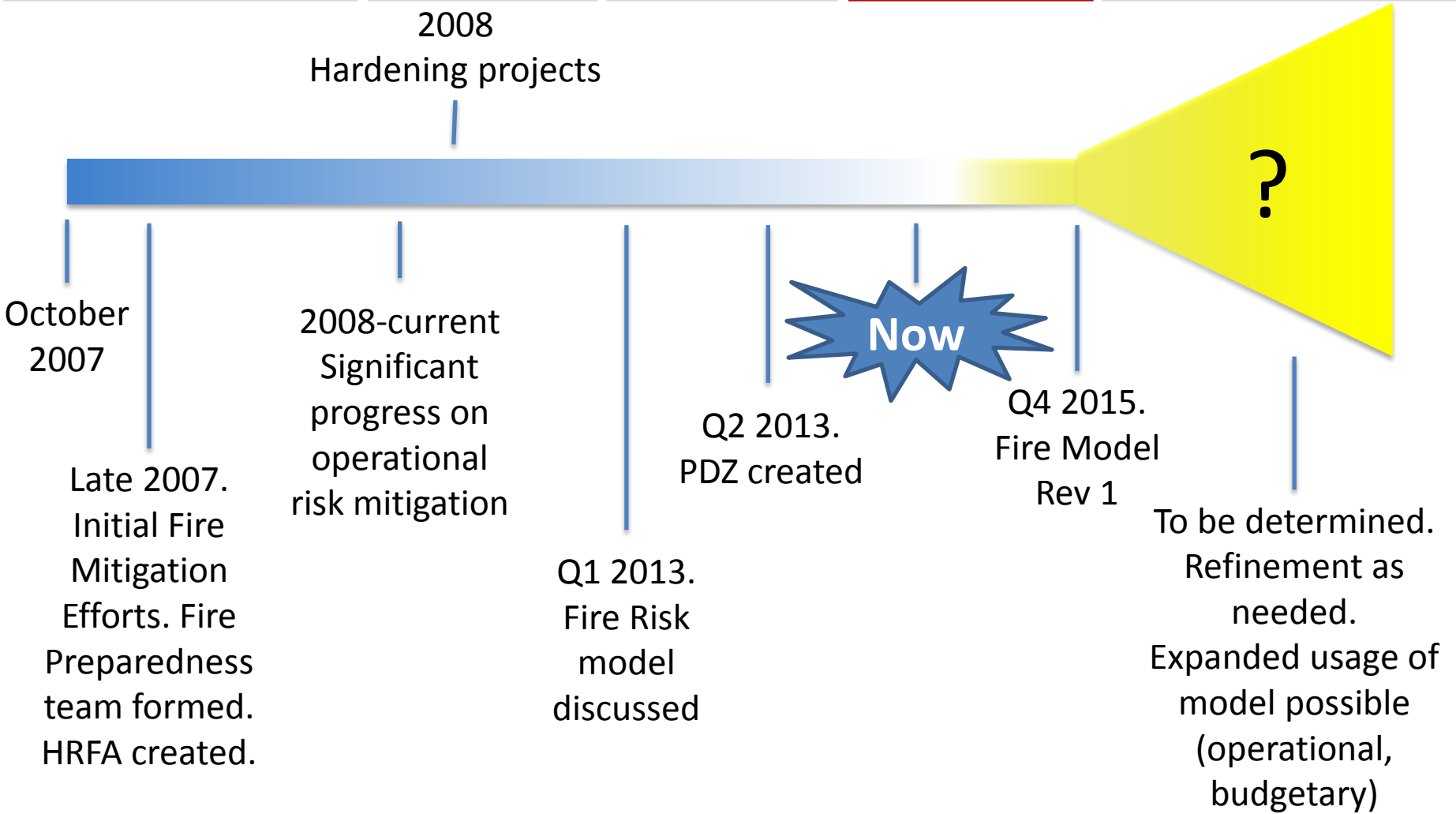
Annual Planning Process

FIRE RISK MANAGEMENT (FIRM)

MASON WITHERS – QUANTITATIVE RISK AND CONTROLS MANAGER



Wildfire Risk Management - Timeline





Wildfire Risk Management - Context

Risk Evaluation Framework

Cybersecurity

TIMP

FiRM

Annual Planning Process

- Operational adjustments were more straightforward; with less budgetary impact, and easier to implement
- System hardening is budgetary and resource intensive
- Fire Risk Mitigation (FiRM) is the Project Management aspect of system hardening for the purposes of risk mitigation
- FiRM focuses on mitigating risk via pole and conductor replacements
- Approximately 3,400 miles of OH distribution system in backcountry. Needed strong, quantitative prioritization method for hardening projects.
- Methods and level of detail may not apply to other risks.



Wildfire Risk Management - Process

Risk Evaluation Framework

Cybersecurity

TIMP

FiRM

Annual Planning Process

- FiRM's prioritization methods are evolving:
 - Original method was created in 2013
 - More quantitative approaches are now forming
 - Fire risk is very complex
 - All prioritizations consider the following fire risk issues:
 - Vegetation
 - Weather
 - Likelihood of Failure Equipment
 - Consequence of ignition
- Fire behavior
-



Wildfire Risk Management - Tool

Risk Evaluation Framework

Cybersecurity

TIMP

FiRM

Annual Planning Process

- Current risk evaluation tool:
 - Potential Damage Zones → Extreme
 - High wind → 85+ MPH wind
 - Higher risk equipment →
 - older #4 and #6 wire
 - wire with many splices
 - poles with wind loading concerns



Wildfire Risk Management - Input



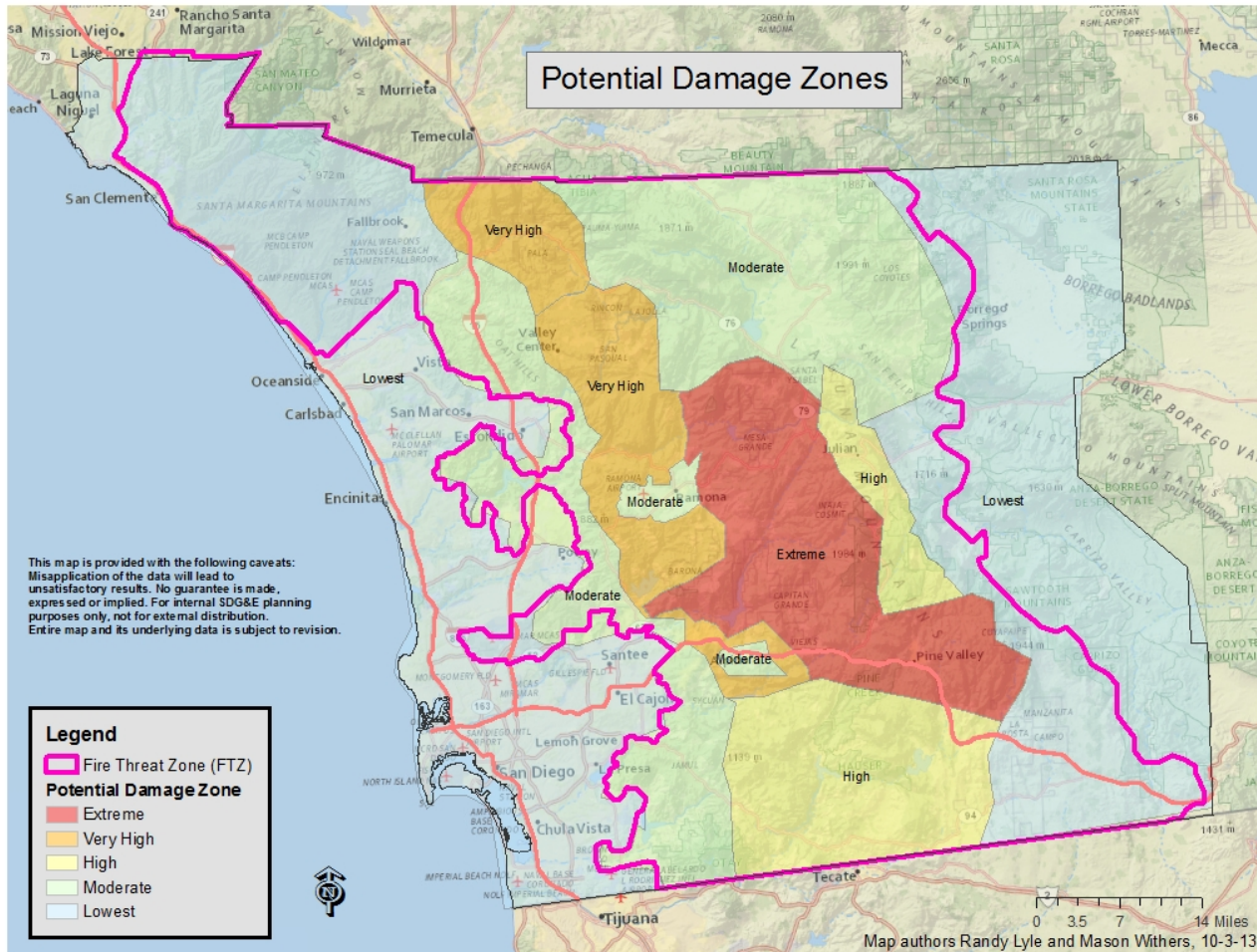
Risk Evaluation Framework

Cybersecurity

TIMP

FIRM

Annual Planning Process





Wildfire Risk Management - Input

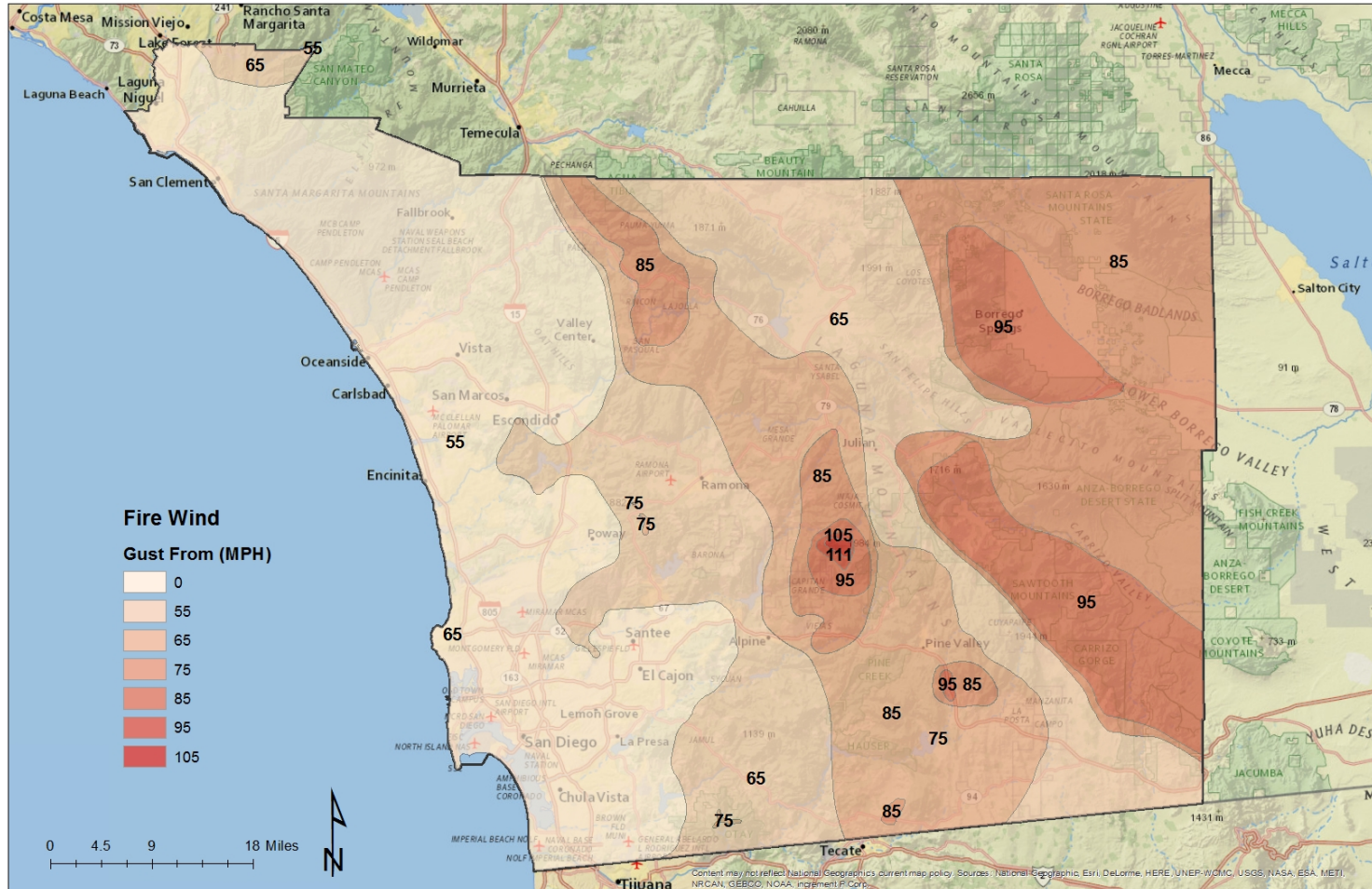
Risk Evaluation Framework

Cybersecurity

TIMP

FIRM

Annual Planning Process





Wildfire Risk Management - Tool

Risk Evaluation Framework

Cybersecurity

TIMP

FiRM

Annual Planning Process

- Wildfire Risk Reduction Model (WRRM)
 - Effort began in 2013. Sought outside consultant; contract signed in Q1 2014.
 - Initial model to focus on equipment failure as trigger & as a prioritization tool for system hardening
 - Utilizes quantitative approach to risk management:
 - Failure Rates (before vs after hardening)
 - Chance of ignition
 - Environmental conditions
 - Fire behavior
 - Consequence
 - Cost of hardening project
 - Risk assessment at every pole, using that pole's characteristics and environmental conditions
 - Performs nearly 70 million fire behavior simulations



Wildfire Risk Management - Illustrative Example

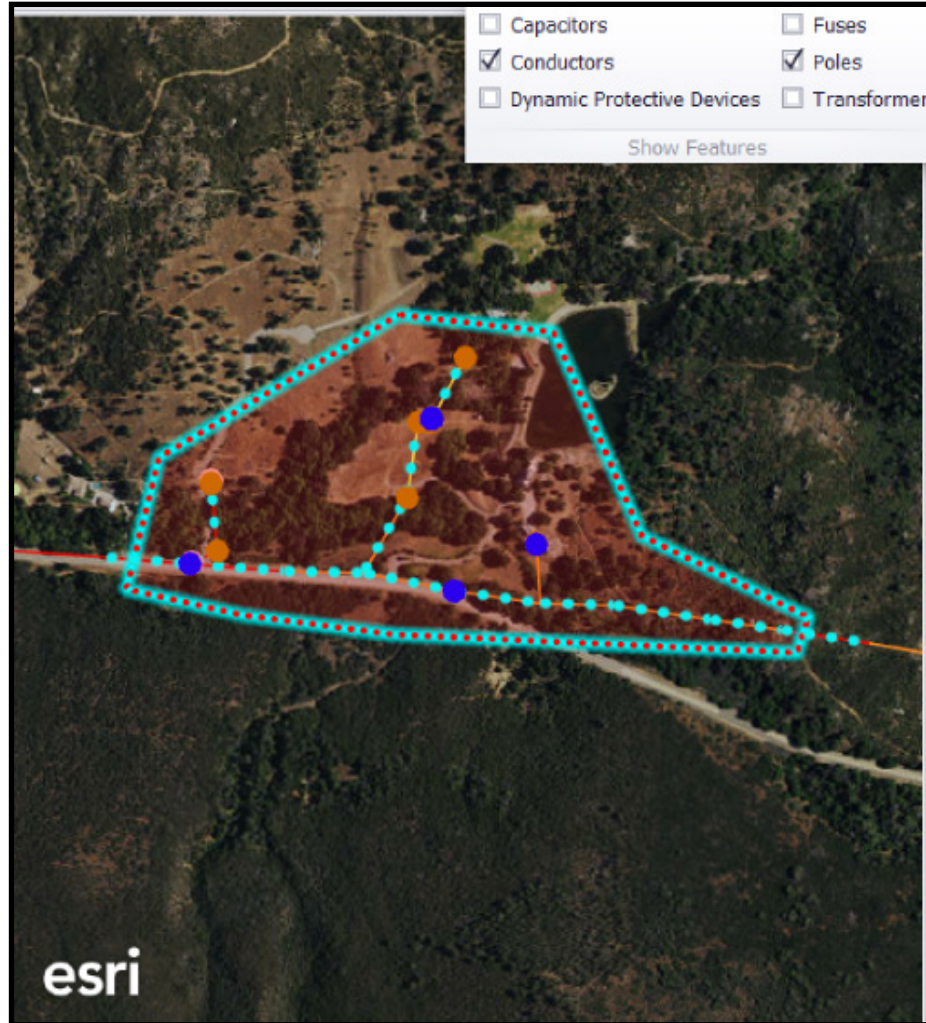
Risk Evaluation Framework

Cybersecurity

TIMP

FiRM

Annual Planning Process





Wildfire Risk Management - Illustrative Example

Risk Evaluation Framework

Cybersecurity

TIMP

FIRM

Annual Planning Process

- Wildfire Risk Reduction Model
 - Can be used to select one project over another
 - Will help define the project scope
 - Requires user control of scenario
- Model is flexible to accommodate future development



Risk Evaluation Framework

Cybersecurity

TIMP

FiRM

Annual Planning Process

ANNUAL PLANNING PROCESS

GREG FLORES – DIRECTOR, ENTERPRISE RISK MANAGEMENT

Annual Planning Process

Risk Evaluation Framework

Cybersecurity

TIMP

FiRM

Annual Planning Process

Monitoring and Review



	Risk Assessment Session	Risk Prioritization Session	Risk Mitigation Planning Session	Investment Planning Process	Risk Mitigation Implementation
Purpose	For each risk owner (officer) to provide an update on the enterprise level risks that they have responsibility for.	To achieve senior management consensus around the relative ranking of risks.	For senior management team to achieve consensus on mitigation priorities which will then be reflected in the 2016 investment planning process.	Allocate investments to manage work and mitigate risks.	Implementation of risk mitigation plans.
Output(s)	Updated risk scoring.	Prioritization of risks the companies are facing.	Preliminary risk mitigation plan to inform upcoming budgeting cycle.	Prioritization of investments.	Implementation of risk mitigation plans.



Discussion

