SAND2010-5678C

Application of Design of Experiments to Security Systems and Technologies Testing

Presented at JMP's Discovery 2010 Conference

September 13 – 15, 2010, Cary, North Carolina

By Kim W. Mitchiner, Ph.D.
Sandia National Laboratories

Co-Authors: Arthur P. Heath, Thomas K. Mack, Larry D. Miller, and Carmella A. Varoz

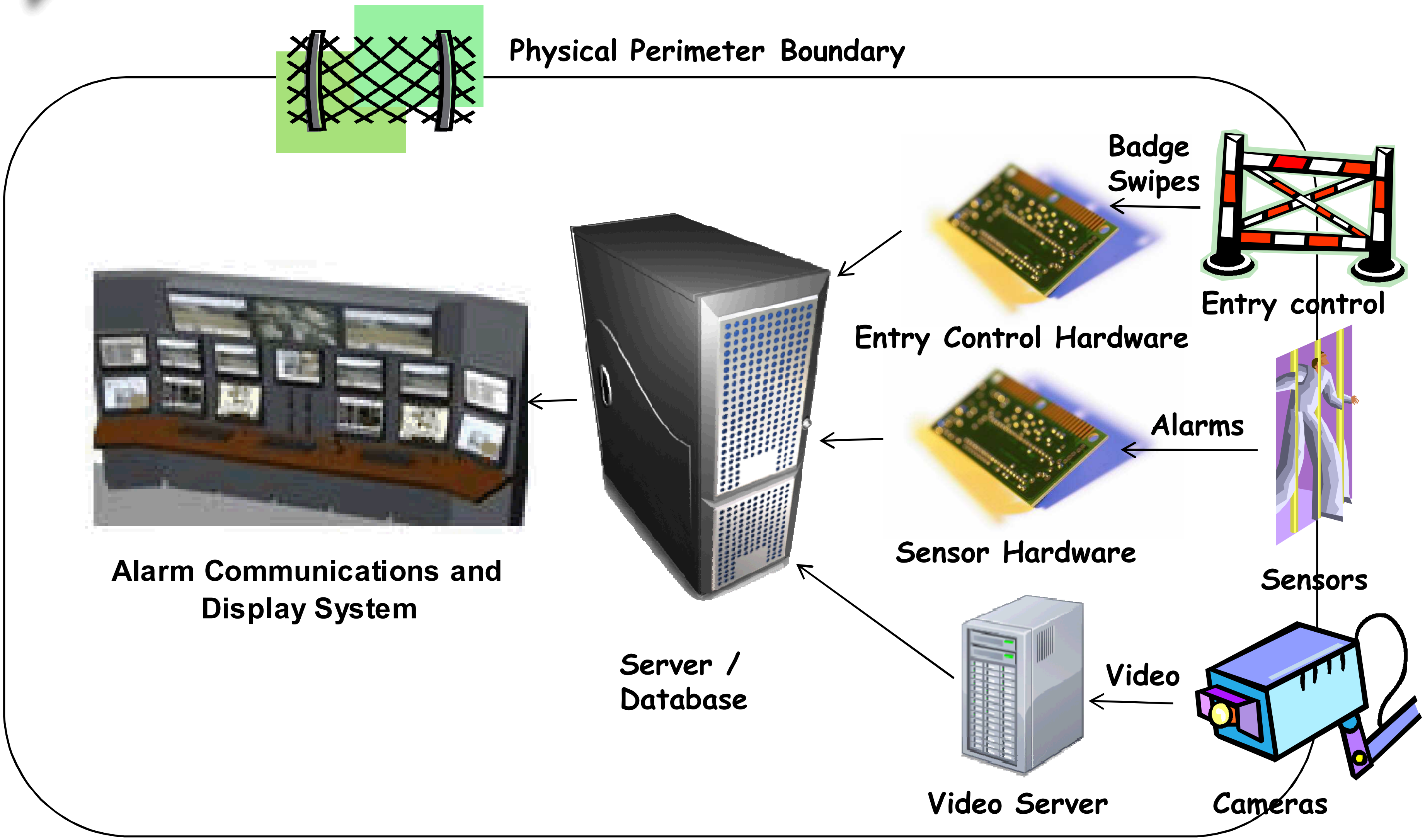
Contact: ☎ (505) 844-2222 : kwmitch@sandia.gov

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Scope of Presentation

- Physical Protection Systems
  - Sensors, Cameras, Entry Control, Alarm Communication & Display (AC&D)
- Design of Experiments
  - Overview
- JMP8® Features Used
- Optimization of Alarm Detection
  - Calibration of a Fiber Optic Intrusion Detection System (FOIDS) sensor
- Entry Control System Performance Evaluation
  - Performance evaluation comparison
  - Identification of systems-level hardware issues

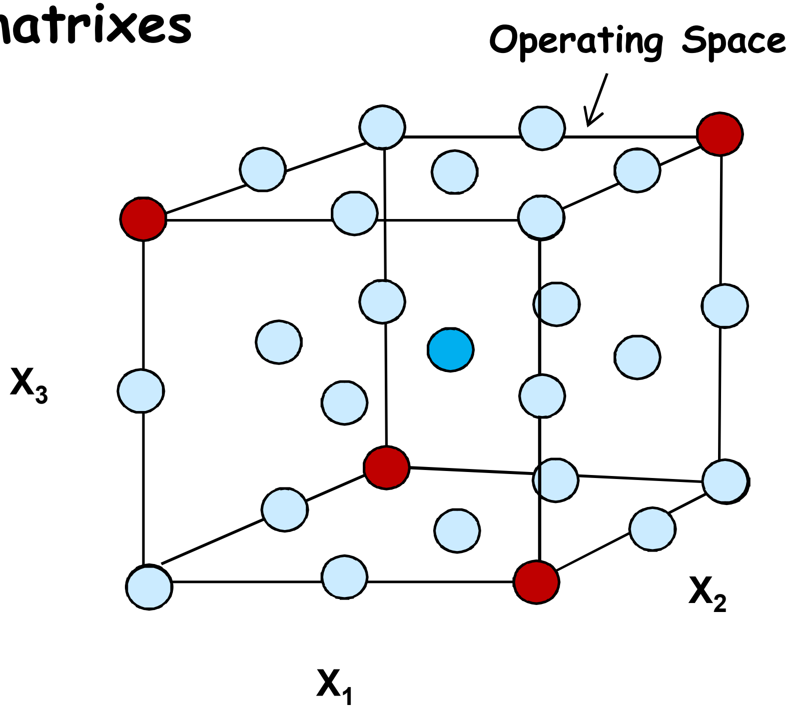
A Physical Security system is a complex system of systems



 Objective: To detect all alarms and entry control transactions

Design of Experiments

- Planned / structured test and evaluation methodology
- Uses statistically designed test matrixes
  - Minimizes number of tests
  - Maximizes information
  - Controls costs
- Yields cause and effect relationships
  - Identifies Significant factors
  - Represents correlations using prediction equations



Can be applied to any multi-variable system with measurable input and output

Three different aspects of the physical security system were studied

- Optimization of alarm detection in the field
  - Physical intrusion cut and climb alarms
- Entry Control System Performance (Authorizations)
  - Badge swipe delays
  - Badge swipe data losses
- Hardware performance for the Entry Control System
  - Correlations between missing badges and hardware performance

JMP8® Features Used

- Optimization of alarm detection in the field
  - DoE custom design
  - Regression analysis (Fit Model)
    - Leverage plots
    - Significant factors
    - Prediction Profiler
  - In the field: Profiler shockwave files

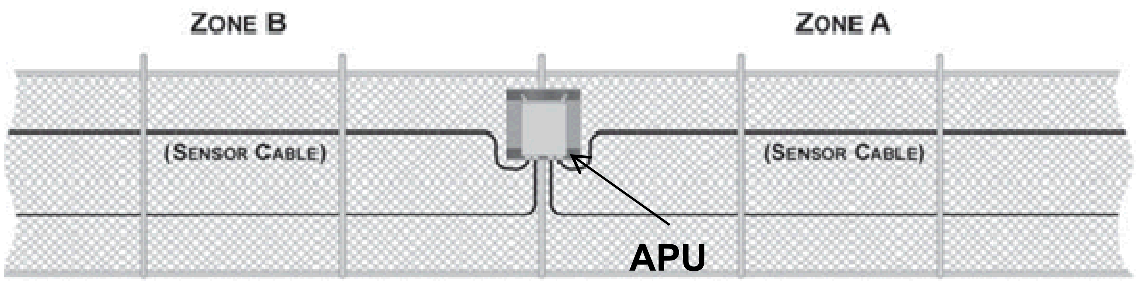
- Entry Control (Authorizations) System Performance
  - DoE
  - Matched Pairs (Wilcoxon signed-rank test)
  - Data mining (Model partitioning)

Physical Security System Evaluations

- Optimization of alarm detection in the field
  - Calibration and optimization of a Fiber Optic Intrusion Detection System (FOIDS) sensor
- Entry Control System Performance
  - to identify a performance issues in an entry control system
- Entry Control Hardware performance
  - to identify a hardware issue in the entry control system

What is a Fiber Optic Intrusion Detection System (FOIDS)?

- Diagram of a fence-mounted High Security FOIDS system

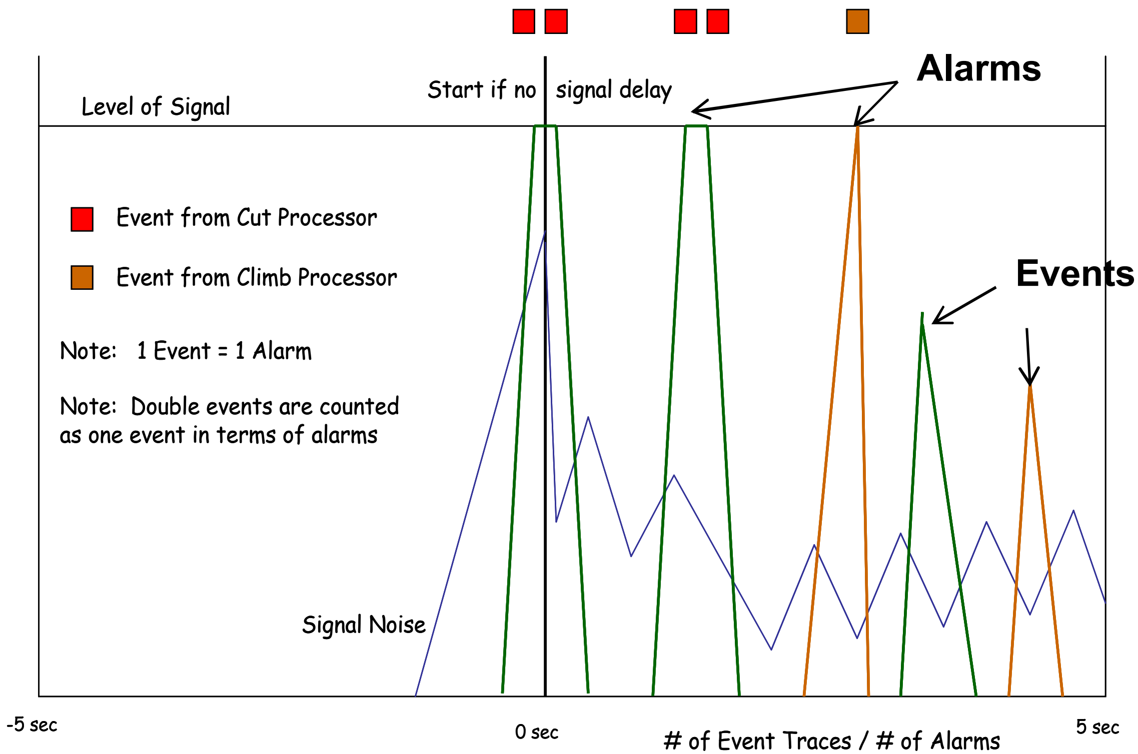


- Designed to identify cut and climb intrusions
- The FOIDS has 32 settings which control alarm detection
- The Alarm Processing Unit has two software processors
  - One processor to detect cut intrusions of the fence fabric
  - One processor to detect climb intrusions on the fence

Sandia National Laboratories

What response was measured to determine detection?

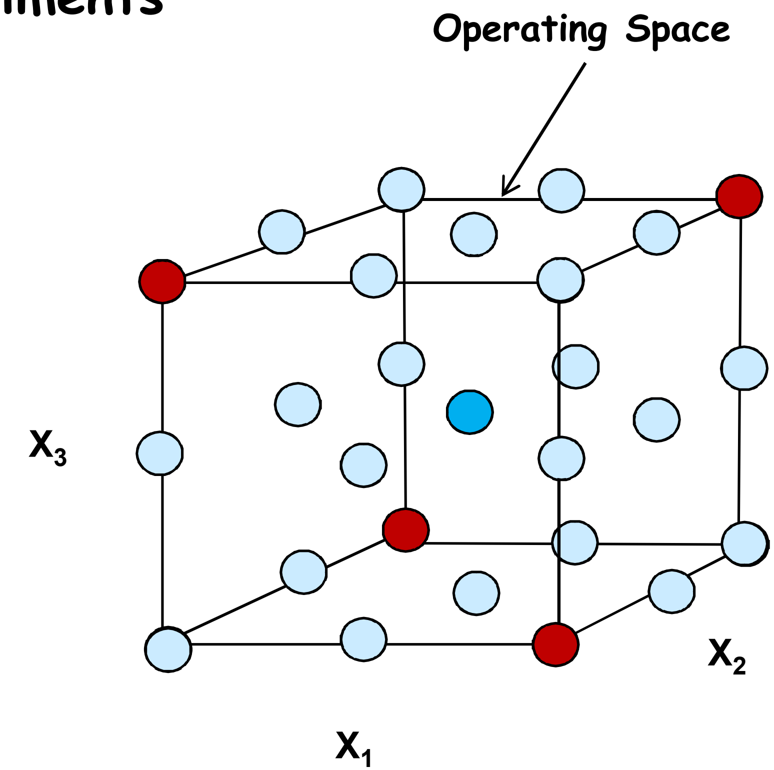
- **Response: The number of alarm events for each intrusion**
- **Typical signal traces for intrusion detections of both cuts and climbs**



Sandia National Laboratories

How to efficiently calibrate the FOIDS in the field for optimum alarm detection?

- Trial and error: inefficient and time-consuming
- Alternative: Design of Experiments
- Approach
  - Fractional Factorial
    - Subset of a full factorial



  - Prediction equation
    - $y = a_0 + a_1x_1 + a_2x_2 + a_3x_3 + (a_{12}x_1x_2 + a_{13}x_1x_3 + a_{23}x_2x_3)$
    - Estimates main effects (and interactions)

The resultant test matrix consisted of 11 settings (factors) and 16 unique experiments

High / low values for each setting bounded the operating space.

Level of Signal Cut	Band pass filter low Cut	Duration of signal Cut	Event mask time Cut	Low Level Tolerance for Cut	Gain	Level of signal Climb	Bandpass filter low Climb	Duration of Signal Climb	Event Mask Time Climb	Low Level Tolerance for Climb
12	400	1	1	3	15	12	300	5	10	5
8	200	5	10	3	15	12	300	5	10	5
8	400	1	10	3	20	8	300	1	1	5
12	400	5	10	3	15	12	500	1	1	5
8	400	1	1	3	15	8	500	5	1	5
8	200	1	10	3	15	12	500	5	1	5
12	400	5	1	3	20	12	300	5	1	5
8	400	5	1	3	15	8	500	1	10	5
12	200	5	1	3	20	8	500	5	1	5
12	200	1	1	3	15	8	300	1	10	5
12	200	5	10	3	15	8	300	1	1	5
8	200	1	1	3	20	12	300	1	1	5
12	200	1	10	3	20	8	500	5	10	5
12	400	1	10	3	20	12	500	1	10	5
8	400	5	10	3	20	8	300	5	10	5
8	200	5	1	3	20	12	500	1	10	5
10*	200*	1*	7*	3*	20*	10*	300*	3*	2*	5*

*Manufacturer's recommended settings

How was testing done in the field?

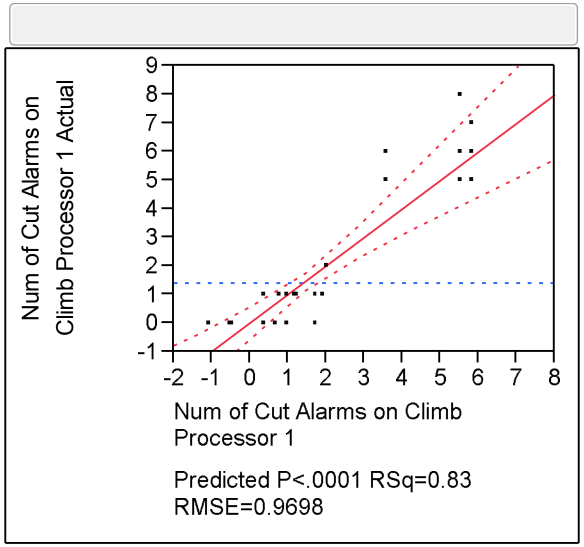
- 16 unique experiments were repeated
  - 2x for climb intrusions
  - 3x for cut intrusions
- Cuts were simulated using a spring loaded tool
  - by one person on single section of the fence
  - 5 simulated cuts were made in 8 sec per test
- Climbs were performed to the top of the 10 ft fence
  - One person
  - Relatively constant climb rate
- To augment the DoE data, additional field data was added to the matrix
- Total experiments
  - 38 climb tests
  - 51 cut tests

What type of statistical analyses were used?

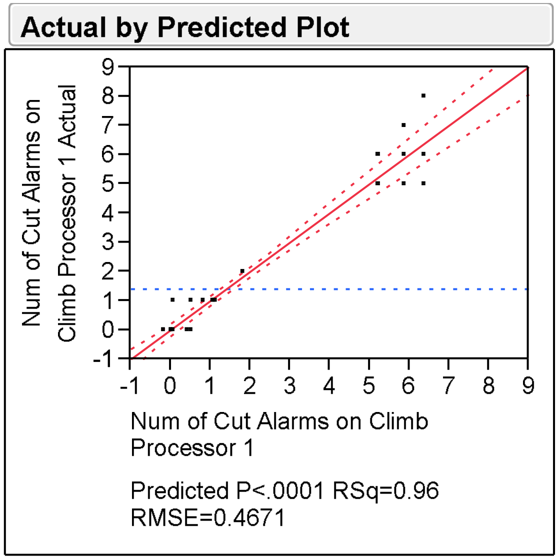
- Regression analysis was used in the JMP8® software to generate 2 cut alarm and 2 climb alarm prediction equations.
  - The cut alarm predicted equations without the interactions had R-sq's of 80%.
  - The cut alarm prediction equations with the unconfounded interactions had R-sq's of 95%.

Cuts Alarms on the Climb Processor

No interactions



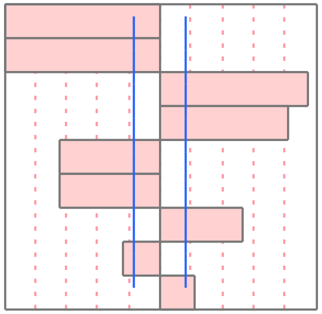
Interactions



What were the significant settings for the cut alarm detection?

- **Cut Processor**

Term	Prob>|t|
Level of Signal Cut	<.0001*
Band pass filter low Cut	<.0001*
(Event mask time Cut-5.86)*(Bandpass filter low Climb-359.4)	<.0001*
(Band pass filter low Cut-305)*(Event mask time Cut-5.86)	<.0001*
Event mask time Cut	<.0001*
Event Mask Time Climb	<.0001*
(Level of Signal Cut-9.92)*(Event mask time Cut-5.86)	<.0001*
Gain	0.0043*
(Band pass filter low Cut-305)*(Event Mask Time Climb-5.44)	0.0090*

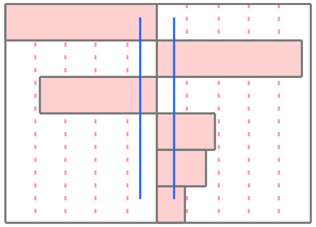


  - Cut and Climb settings were significant for cut alarm detection on the cut processor

Actual by Predicted Plot

- **Climb Processor**

Term	Prob>|t|
Event Mask Time Climb	<.0001*
(Duration of Signal Climb-3.16)*(Event Mask Time Climb-5.44)	<.0001*
Duration of Signal Climb	<.0001*
(Level of signal Climb-9.9)*(Bandpass filter low Climb-359.4)	<.0001*
Low Level Tolerance-climb	<.0001*
(Gain-17.78)*(Duration of Signal Climb-3.16)	0.0033*



Sandia National Laboratories

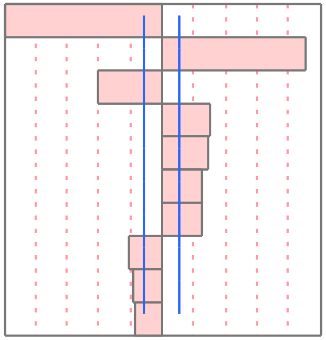
What were the significant settings for climb alarm detection?

- **Cut settings and climb settings were significant for detection on both processors**

- **Climb processor**

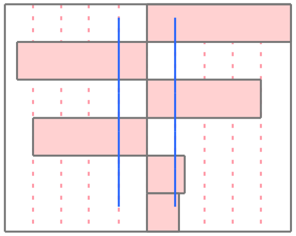
Prob>|t|

Term	**Prob>|t|**
Duration of Signal Climb	<.0001*
(Duration of Signal Climb-3.10526)*(Event Mask Time Climb-5)	<.0001*
Event Mask Time Climb	<.0001*
Duration of signal Cut	<.0001*
(Level of Signal Cut-9.73684)*(Event Mask Time Climb-5)	<.0001*
Level of Signal Cut	0.0001*
(Duration of signal Cut-2.47368)*(Event Mask Time Climb-5)	0.0002*
(Level of Signal Cut-9.73684)*(Duration of Signal Climb-3.10526)	0.0010*
Low Level Tolerance - climb	0.0039*
Location middle (1) or post (0)	0.0063*



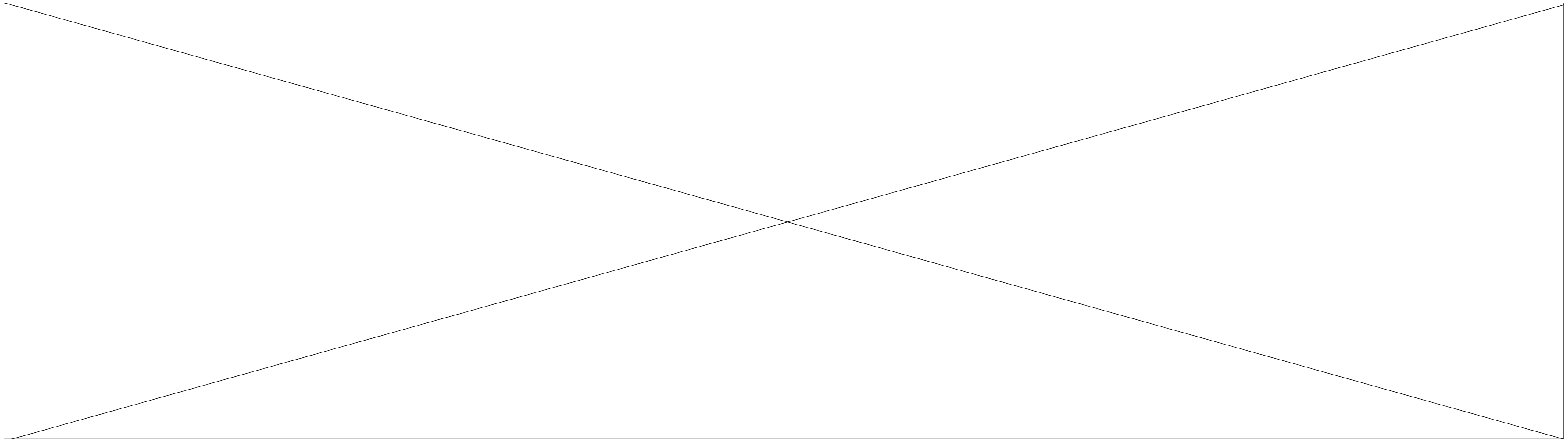
- **Cut processor**

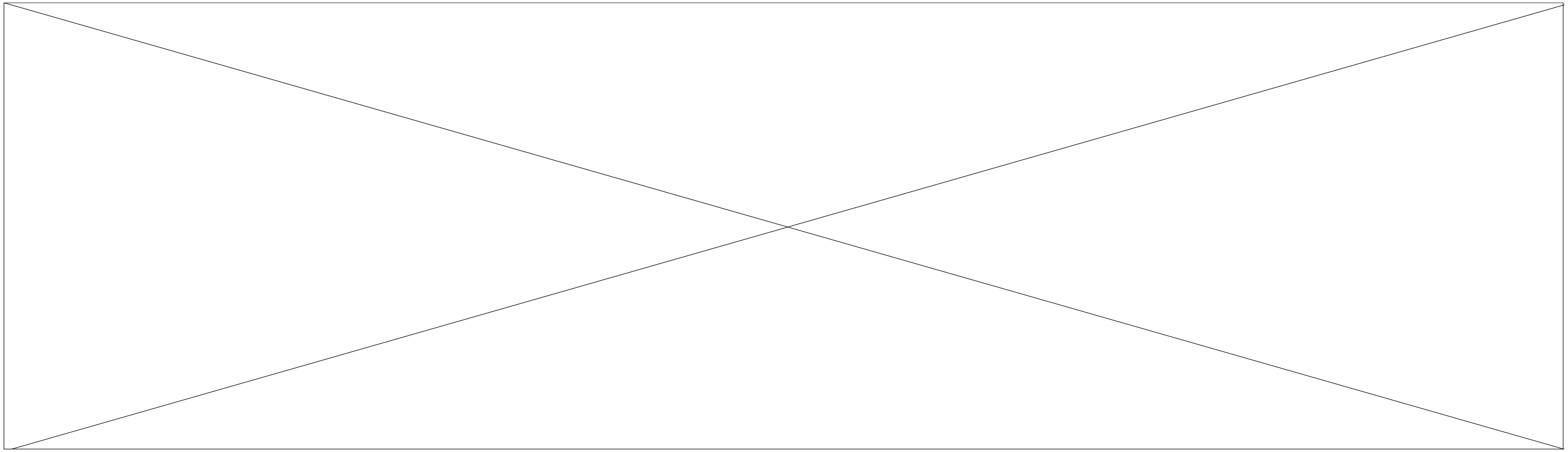
Term	Prob>|t|
(Event mask time Cut-5.89474)*(Duration of Signal Climb-3.10526)	<.0001*
Event Mask Time Climb	<.0001*
(Event mask time Cut-5.89474)*(Event Mask Time Climb-5)	<.0001*
Duration of Signal Climb	<.0001*
(Duration of signal Cut-2.47368)*(Gain-17.5789)	0.0103*
(Location middle (1) or post (0)-0.52632)*(Level of signal Climb-9.89474)	0.0341*



Optimization of all four prediction equations together was required to calibrate the FOIDS

The objective: no alarms on the "wrong" processors; real alarms on the "right" processors for either cuts or climbs. (Pictures are of plots of prediction equation lines by factor)





***The shockwave files shown here can be transferred to the field for real time optimization**

Was it possible to identify more than one group of optimal settings?

Test Type	Level of Signal Cut	Bandpass filter freq low Cut	Duration of signal Cut	Low level tolerance - cut	Event mask time Cut	Gain	Level of signal Climb	Bandpass filter freq low Climb	Duration of Signal Climb	Event Mask Time Climb	Low Level Tolerance-climb	Predicted Num of Cut Alarms on Climb Processor	Predicted Num of Cut Alarms on Cut Processor	Predicted Num of Climb Alarms on Cut Processor	Predicted Number of Climb Alarms on Climb Processor
JMP - 4 equation optimization with interactions	11	245	3	3	6	18	11	195	5	3	4	-0.9	1.5	-0.2	3
Genetic Algorithm - 4 equation optimization-main factors only	10	200	4	3.5	3	19	12	153	2	6	4	0.5	1.8	0.5	2
Manufacturer's Recommended	10	200	1	3	7	20	10	300	3	2	5	3	2	1	0.8
Validation															
Cut (actual)	8	400	1	3	1	15	8	500	5	1	5	0	1		
calc (2 eqn - pred)												0	1		
Cut (actual)	10	200	1	3	7	22	12	140	3	2	4	0	1		
calc (2 eqn - pred)												0.5	1.3		
Climb (actual)	8	400	1	3	10	20	8	300	1	1	5			0	5
calc (2 eqn - pred)														0.6	6.1
Climb (actual)	12	200	5	3	10	15	8	300	1	3	5			0	7
calc (2 eqn - pred)														0.6	6.3
Examples of alternative settings															
Climb 2 equation	10	200	3	3	2	17	10	350	5	6	4			-0.9	2
Cut 2 equation	"	"	"	"	"	"	"	"	"	"	"	-0.5	3.8		
Climb 2 eqn pred	11	250	2	3	2	16	12	400	4	4	4			-0.2	2.4
Cut 2 eqn pred	"	"	"	"	"	"	"	"	"	"	"	0.5	1.9		
Climb 2 eqn pred	12	300	2	3	2	18	12	200	4	4	4			-0.5	2.2
Cut 2 eqn pred	"	"	"	"	"	"	"	"	"	"	"	-0.3	4		

* (JMP - 4 equation optimization with interactions)

Actual vs. pred. Cut alarms

Actual vs. pred. Climb alarms

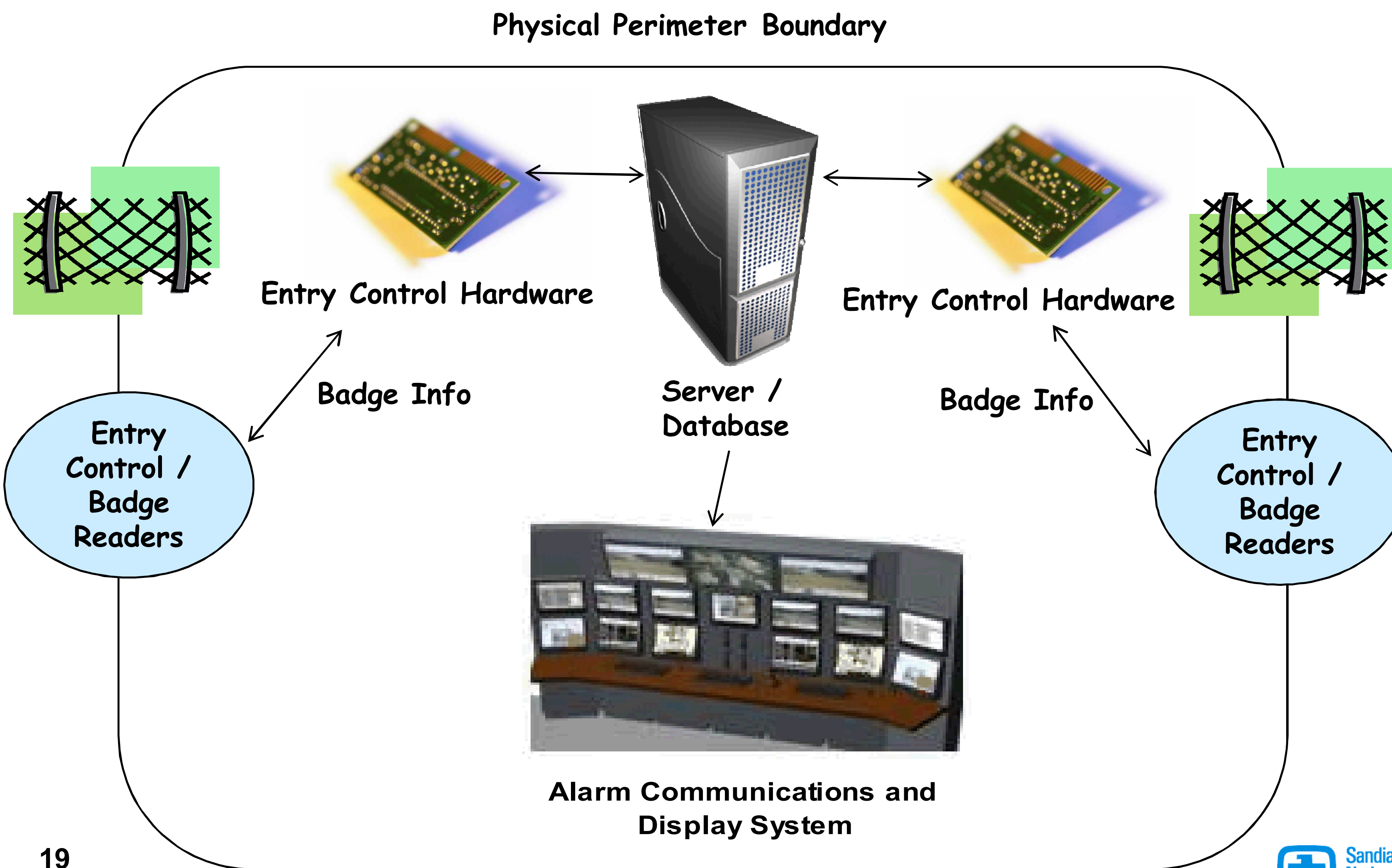
* (Examples of alternative settings)

* Recommended

Physical Security System Evaluations

- Optimization of alarm detection in the field
  - Calibration and optimization of a Fiber Optic Intrusion Detection System (FOIDS) sensor
- Entry Control System performance comparisons
  - to identify a performance issues in an entry control system as a function of software upgrades
- Entry Control Hardware performance evaluation
  - to identify a hardware issue in the entry control system

Schematic of an Entry Control System



Step 1: Use DoE to evaluate systems level performance of the Entry Control System

- System consisted of over 16 main components
  - Servers / database
  - Hardware / Software
- Numerous database software upgrades were being made
  - This had a direct impact on entry control transactions
- Needed a systems-level protocol for testing performance
  - Design of experiments (DoE)
    - Selected as a standardized method of testing between software and hardware upgrades
- Because of applying DoE and other statistics
  - software-related and hardware-related performance issues were identified

Performance Test Matrix for Entry Control consisted of 21 unique experiments

Resolution III test matrix with 11 factors (5 centerpoints)

Hardware factors: SCP7b, SCP8b, MR5217, MR5227, MR5218, MR5228

SPA Relay Events *	Total Vendor Alarm Events *	Duration	NumofBadges	ECOPsFreq	SCP7b	SCP8b	MR5217	MR5227	MR5218	MR5228
30	335	10	1000	10	1	1	2	1	2	1
0	343	5	1000	3	1	1	2	1	2	1
12	77	10	1000	3	1	0	2	1	0	0
0	361	5	5000	3	1	1	2	1	2	1
60	182	5	1000	10	1	0	1	0	0	0
0	51	5	1000	3	0	1	0	0	1	0
0	421	10	5000	10	1	1	1	0	2	0
30	160	5	5000	3	1	0	2	1	0	0
0	126	5	5000	10	1	0	1	0	0	0
30	30	10	5000	10	1	0	0	1	0	0
0	26	10	1000	3	1	0	1	0	0	0
0	53	10	1000	10	0	1	0	0	1	0
15	52	5	1000	3	0	1	0	0	2	1
0	214	10	5000	10	0	1	0	0	2	1
24	379	10	5000	3	1	1	2	1	2	1
0	69	5	5000	10	1	0	1	0	0	0
0	30	5	1000	3	0	1	0	0	0	1
0	173	5	1000	10	0	1	0	0	2	1
0	370	5	1000	10	1	1	2	1	2	1
24	50	10	5000	3	0	1	0	0	1	0
30	338	5	1000	3	1	1	2	1	2	1

* Uncontrolled factors

How was the performance assessed?

- Performance was measured by determining
  - Entry control data losses
  - Entry control delays

- Measurements were made at millisecond rates during the 30 second runs

- As a result, averages of the data were used in the comparisons
  - *Average Absolute Deviation (AAD)** of the Entry Control Transactions (data losses)
  - *Average Absolute Deviation (AAD)** of the Entry Control Responses (data delays)

*Avg Absolute Deviation was used to reduce sensitivity of the analysis to outliers.

The "Fit Model" tool was used to identify the significant factors

- Tests were performed before the software upgrades and after the upgrades
- Significant factors based on regression analysis

Significant factors in Entry Control System Performance								
				Hardware				
	No. of Badges in DB	Frequency of Entry	Duration of EC transaction	MR 52-17	MR 52-27	MR52-18	MR52-28	Alarms
Entry Control data loss								
- pre-upgrade	X	X		X	X	X	X	
- post-upgrade	X		X	X	X		X	
Entry Control data delay								
- pre-upgrade							X	X
- post-upgrade						X		

- Hardware was a consistent issue with both pre-and post-upgrades, especially for Entry Control data loss

Knowing the significant factors, did not tell us whether performance had improved

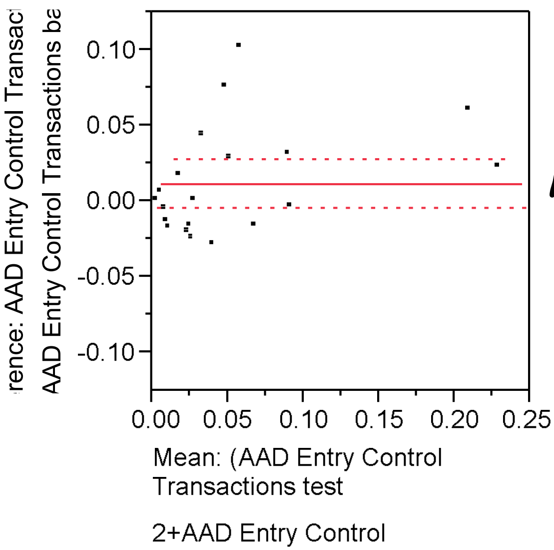
- To determine if there were changes in performance
  - "Matched Pair" tool in JMP8®
  - Wilcoxon signed-rank (matched pair) tests in JMP8®

- Two metrics were considered
  - Average Absolute Deviation* of the Entry Control Transactions, i.e. data loss
  - Average Absolute Deviation* of the Entry Control Response, i.e. data delay

*Avg Absolute Deviation was used to reduce sensitivity of the analysis to outliers.

The "Matched Pairs" tool was used to assess differences in performance

Entry Control Data Loss

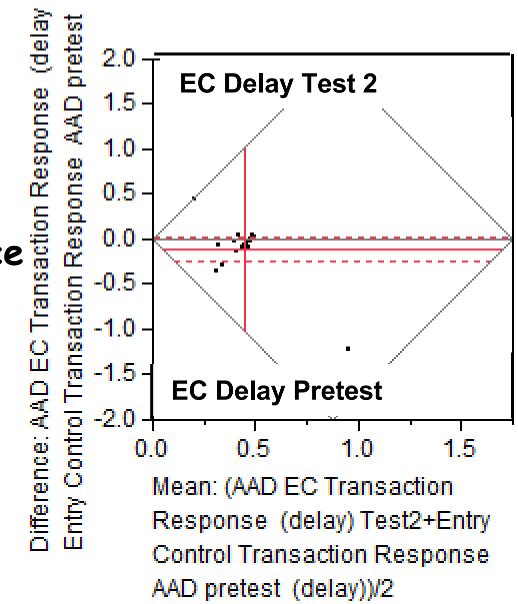


y2 < y1

Mean difference

y2 > y1

Entry Control Data Delay



Prob>|t|

No significant difference in data loss performance

Definite difference in delay performance

Sandia National Laboratories

Wilcoxon Signed-Rank test* identified whether improvements occurred

* Nonparametric version of the paired t-test

- Entry control data loss performance

	AAD Entry Control Transactions test 2-AAD Entry Control Transactions baseline
Test Statistic	28.500
Prob > |z|	0.3339
Prob > z	0.1670
Prob < z	0.8330

No improvement

Difference is not significant

- Entry control data delay performance

Wilcoxon Sign-Rank

Transactions baseline)/2

	AAD EC Transaction Response (delay) Test2-Entry Control Transaction Response AAD pretest (delay)
Test Statistic	-83.500
Prob > |z|	0.0016*
Prob > z	0.9992
Prob < z	0.0008*

Definite improvement in delay times

Difference is significant

Software upgrades only influenced the Entry Control delay times

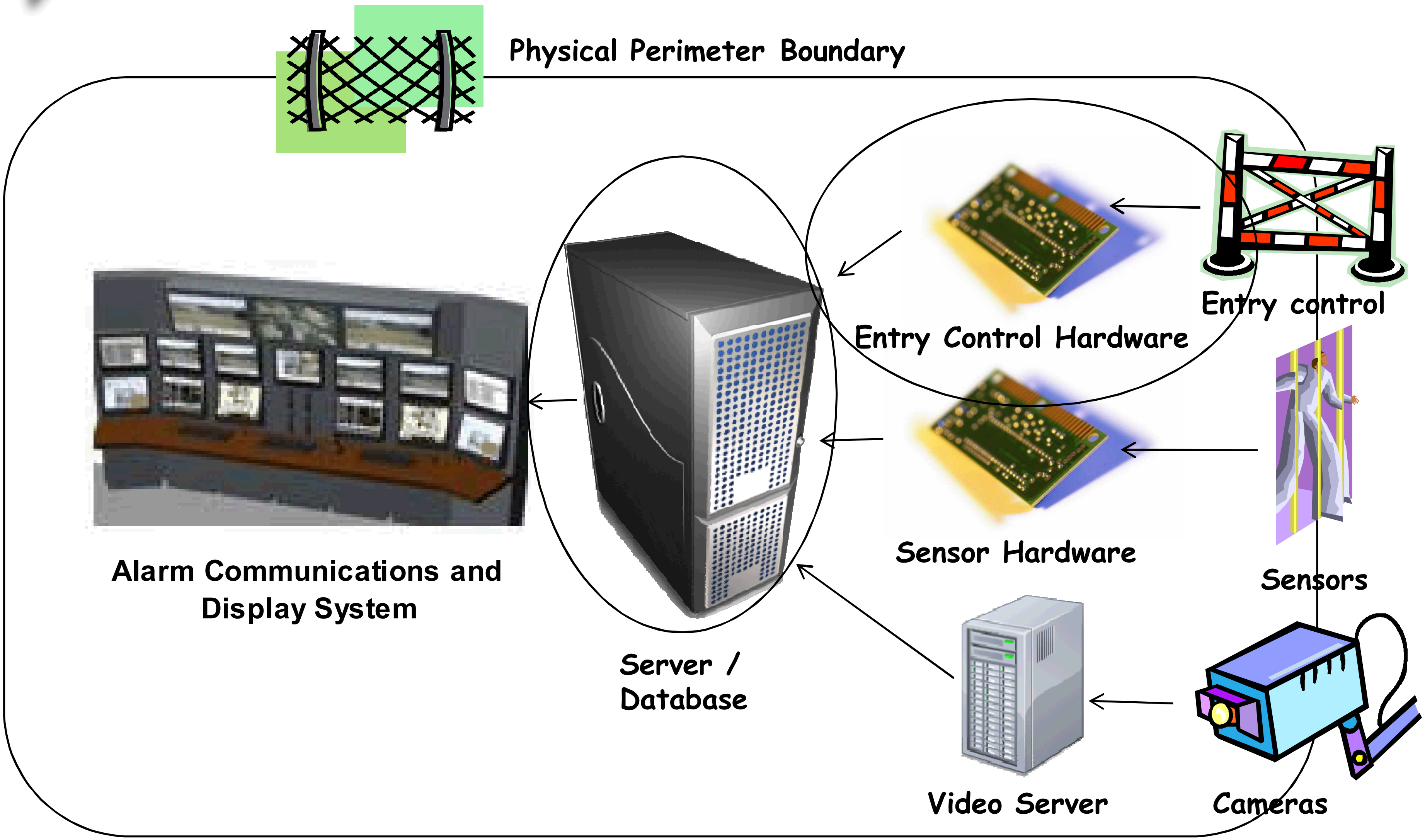
- Significant factors identified badge transaction factors and hardware factors were influencing the data losses
- Significant factors for data delays indicated only a hardware component.
- The "Match Pair" tool plot indicated
  - Definite difference in performance- Entry Control delay times
- Wilcoxon signed-rank paired test identified whether performance had improved
  - Improvements were only noted for Entry Control delay

- What was the source of the Entry Control data losses?

Physical Security System Evaluations

- Optimization of alarm detection in the field
  - Calibration and optimization of a Fiber Optic Intrusion Detection System (FOIDS) sensor
- Entry Control System performance comparisons
  - to identify a performance issues in an entry control system as a function of software upgrades
- Entry Control Hardware performance evaluation
  - to identify a hardware issue in the entry control system

Entry Control data losses appeared to be hardware related



Objective: To detect all alarms and entry control transactions

- A larger designed test matrix was required to evaluate the hardware in the system
  - 8 variables
  - 56 tests with 10 random replicates and 5 centerpoints (total of 66 tests)
  - Randomized test sequence

- Used JMP8®'s data mining capability to evaluate entry control data losses
  - Looked at different hardware components
    - Hardware components DSTED's 9,10,13,16
    - Associated badge reader ports 0, 1, 2 on each hardware board

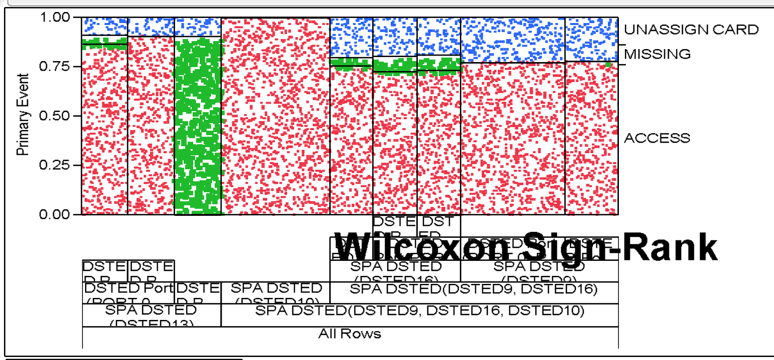
Hardware effects were evaluated as response data

- Excerpt from 66 test matrix

Test	Test	Number of Card Readers	Badge Range	ECOps Freq	Process/HW Alloc	Video	SCP Faults	Number of Alarms	Unassigned badges
15	25	3	1000	12	1	1	0	3	0
16	29	7	3000	20	1	0	0	16	1
17	30	12	5000	12	1	0	0	30	0
18	32	3	1000	30	1	0	1	30	0
19	37	12	1000	30	1	0	1	30	1
20	30	12	5000	12	1	0	0	30	0
21	43	3	5000	30	1	1	1	30	0
22	45	12	5000	12	1	1	1	3	1
23	51	3	5000	30	1	0	0	30	0
24	52	12	1000	12	1	0	1	3	1
25	53	12	1000	30	1	0	0	3	1
26	54	3	5000	12	1	0	1	3	0
27	51	3	5000	30	1	0	0	30	0
28	55	3	5000	30	1	1	1	3	1
29	1	3	5000	30	2	0	0	3	0
30	7	12	5000	30	2	0	1	30	1

- Response: # missing, assigned, and unassigned badges by hardware component and badge reader port

Partitioning of data points indicated that Missing badges were occurring primarily on DSTED 13, badge reader Port 2

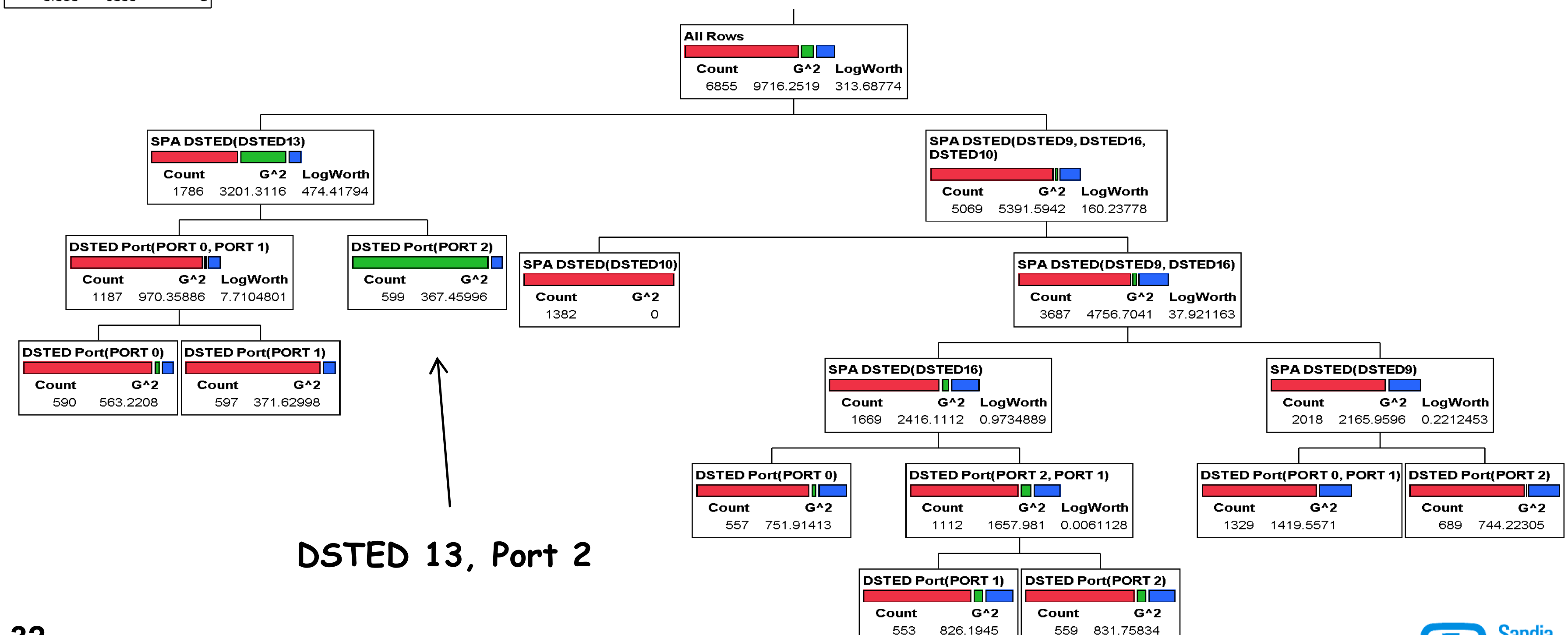


Unassigned

Missing

Assigned

RSquare	N	Number of Splits
0.395	6855	8



DSTED 13, Port 2

Results of the data partitioning

- Without the used of data mining coupled with DoE, it may not have been possible to identify the suspect hardware
  - Hardware component DSTED 13 with card reader port 2 accounted for the majority of the missing badges (8% out of a total of 10%)
  - The remaining 2% were associated with Hardware component DSTED 16, all badge reader ports and DSTED 9 Port 2
  - After replacement of the DSTED 13 hardware board,
    - 1.5% total missing badge transactions still occurred randomly
    - The remaining missing transactions were not localized on any specific boards

Summary

- Variety of statistical, DoE, and data mining tools in JMP8® were applied to different physical security systems
  - Each application was multi-variable and complex
  - Each application had measurable input and output
- The applications included
  - Optimization of alarm detection in the field
    - DoE custom design, Fit Model, and Prediction Profiler tools were used to identify optimum setting combinations in the field
  - Entry Control System performance comparisons
    - "Matched Pairs" and the "Wilcoxon signed-rank test" were used to identify "if" a change had occurred and "whether there were improvements"
  - Entry Control Hardware performance evaluation
    - The "Partition Model" tool was used to sort through and classify system components involved in performance issues

Questions??

kwmitch@sandia.gov 505-844-2222

Backup slides

Setting interactions had a significant influence on alarm detection in the FOIDS

Partition for Primary Event

RGE6

Cut Alarms on the Cut Processor

11.3773819485206
+-0.5106593614073*Level of Signal Cut
+-0.0069437147511*Band pass filter low Cut
+-0.1269416991706*Event mask time Cut
+-0.0781511972864*Gain
+-0.1161280495989*Event Mask Time Climb
+ (Level of Signal Cut-9.92) * ((Event mask time Cut-5.86) * 0.05049586463938)
+ (Band pass filter low Cut-305) * ((Event mask time Cut-5.86) * 0.00169047136143)
+ (Band pass filter low Cut-305) * ((Event Mask Time Climb-5.44) * 0.00039013659732)
+ (Event mask time Cut-5.86) * ((Bandpass filter low Climb-359.4) * 0.00243407569164)

Cut Alarms on the Climb Processor

Prediction Expression

-0.9156921505773
+-0.6079927761089*Duration of Signal Climb
+-0.2920421439693*Event Mask Time Climb
+ 1.25746286332251 * Low Level Tolerance-climb
+ (Gain-17.78) * ((Duration of Signal Climb-3.16) * 0.04463061186677)
+ (Level of signal Climb-9.9) * ((Bandpass filter low Climb-359.4) * 0.00267516601494)
+ (Duration of Signal Climb-3.16) * ((Event Mask Time Climb-5.44) * 0.1348908398865)

Interactions across processors were particularly important.

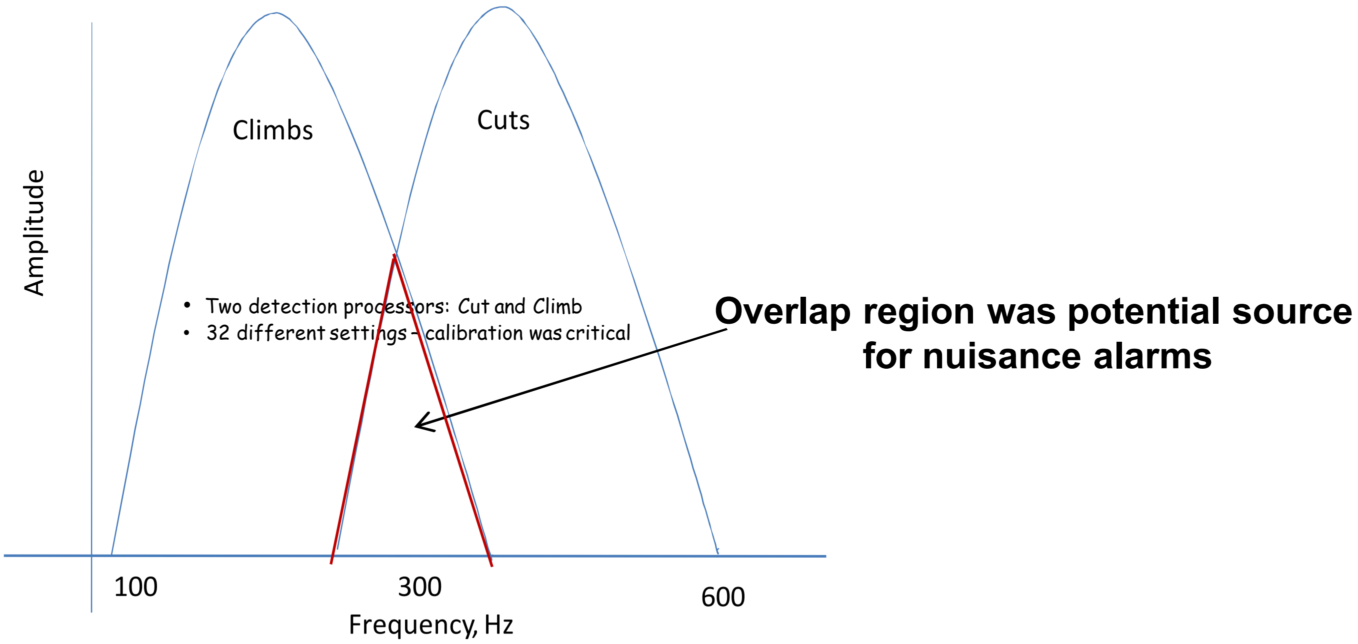
Sandia National Laboratories

Slide 37

RGE6 I definitely wouldn't show all these prediction equations with umpteen digits.
Robert Easterling, 6/23/2010

The objective of the testing was to calibrate the FOIDS for alarm detection with minimum nuisance alarm rate

- **During field testing for cut and climb intrusions, intrusion alarms were found to be occurring on both processors**
- **This overlap region in the frequency plot was suspected to be contributing to the nuisance alarm rates (NAR's)**



Sandia National Laboratories

The prediction equations were used to identify the sensitivity of alarm detection to changes in the significant factors

The steepness of the slope of the lines shows the sensitivity of alarm detection to changes in the setting values

For Climb alarm detection, duration of signal cut and level of signal cut are the most sensitive

Interactions between processor settings further complicated the calibration.