26th annual INCOSE international symposium
Edinburgh, UK
July 18 - 21, 2016

System Engineer Design Support via System Dynamics Modeling of Cybersecurity Operations

Presenter: Keith D. Willett, CISSP, ISSAP
Enterprise Security Architect, DoD
PhD Candidate at Stevens Institute of Technology

Agenda

26th annual INCOSE international symposium
Edinburgh, UK
July 18 - 21, 2016

- The Problem
- A Solution
  - Solution Approach
  - Strategic & Tactical Context
  - The Model
  - Conclusions
  - Future

The Problem

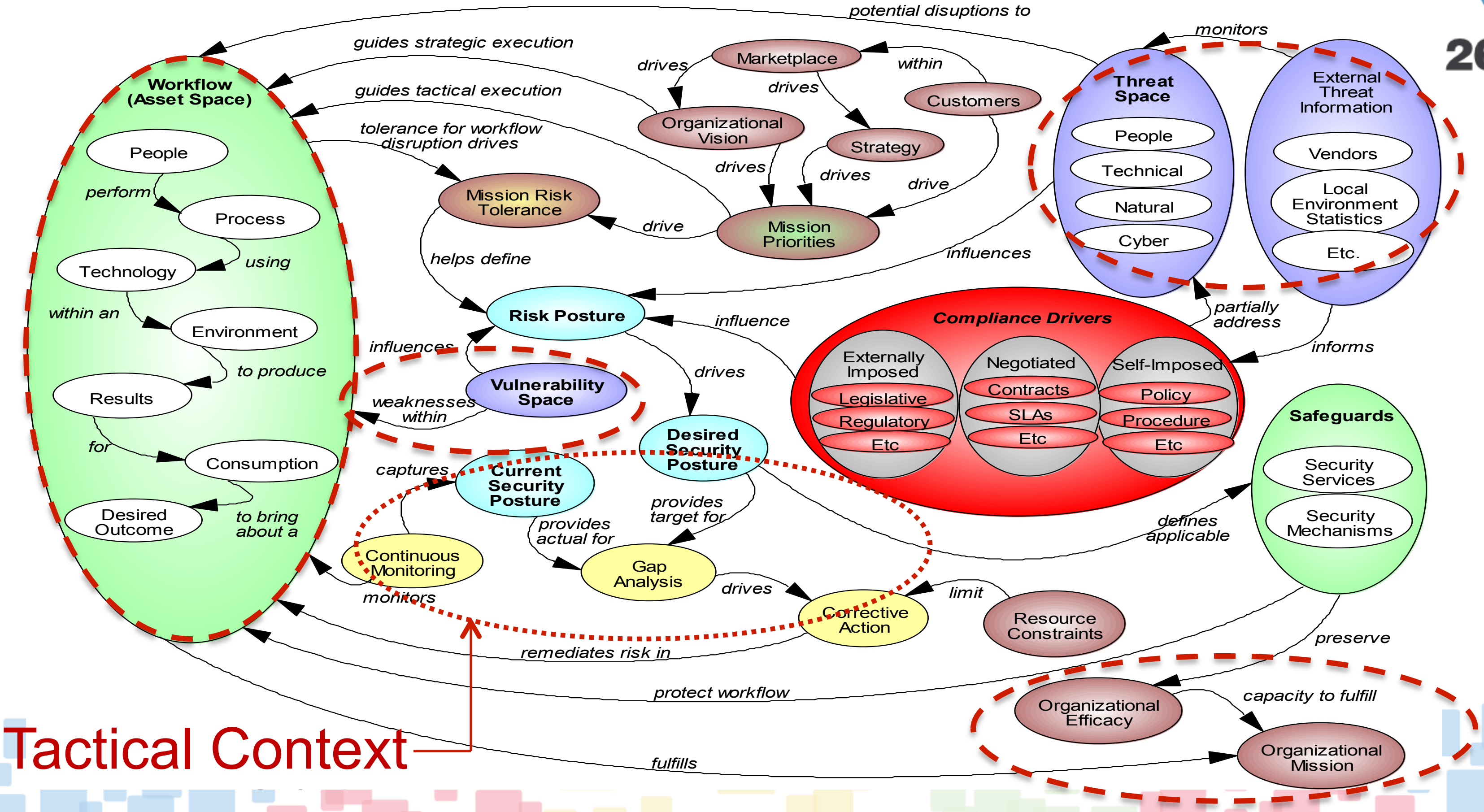
Lack of systems engineering (SE) decision support for tradeoff analysis in system of systems (SoS) design.

ModSim Approach

- **Type**: system dynamics modeling (SDM)
- **Tool**: STELLA/iThink
- **Focus**: cybersecurity operations, anomaly processing
- **Perspective**: quantity and time of anomalies processed
- **Intent**:
  - Discern baseline of quantity and time
  - Find fit of prospective solution
  - Determine impact
  - Modify model according to projected effects
  - Compare results to baseline for localized and systemic effect
- **Case Study**: cybersecurity decision patterns (CDPs) as one proposed solution under *Integrated Adaptive Cyberspace Defense* (IACD)

Strategic Context

26th annual INCOSE international symposium
Edinburgh, UK
July 18 - 21, 2016



Tactical Context

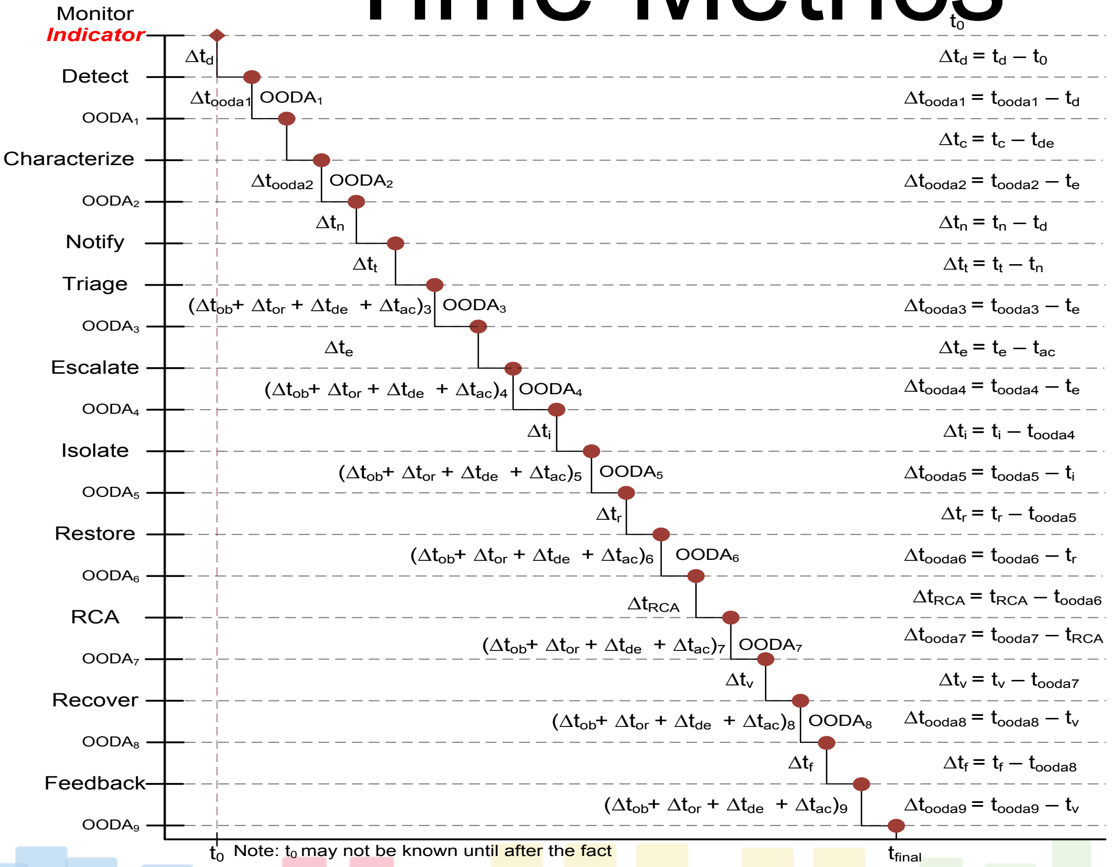
Tactical Context

(Cybersecurity Operations Workflow Phases)

26th annual INCOSE international symposium
Edinburgh, UK
July 18 - 21, 2016

1. **Monitor**: ongoing observation with intent to raise awareness
2. **Detect**: indicator of anomaly
3. **Characterize**: known-known, known-unknown, unknown-unknown, unknown-known
4. **Notify**: first tier support
5. **Triage**: determine priorities
6. **Escalate**: send to subject matter expert
7. **Isolate**: contain threat or threat effects
8. **Restore**: restore effective operations even at diminished efficiency
9. **Root Cause Analysis**: identify root cause of problem
10. **Recover**: recover effective & efficient operations to desired performance level
11. **Feedback**: minimize recurrence and effects of recurrence

Time Metrics


t_0
Monitor
Indicator
Detect
OODA₁
Characterize
OODA₂
Notify
Triage
OODA₃
Escalate
OODA₄
Isolate
OODA₅
Restore
OODA₆
RCA
OODA₇
Recover
OODA₈
Feedback
OODA₉
Δt_d
Δt_{ooda1} OODA₁
Δt_{ooda2} OODA₂
Δt_n
Δt_t
$(\Delta t_{ob}+ \Delta t_{or} + \Delta t_{de} + \Delta t_{ac})_3$ OODA₃
Δt_e
$(\Delta t_{ob}+ \Delta t_{or} + \Delta t_{de} + \Delta t_{ac})_4$ OODA₄
Δt_i
$(\Delta t_{ob}+ \Delta t_{or} + \Delta t_{de} + \Delta t_{ac})_5$ OODA₅
Δt_r
$(\Delta t_{ob}+ \Delta t_{or} + \Delta t_{de} + \Delta t_{ac})_6$ OODA₆
Δt_{RCA}
$(\Delta t_{ob}+ \Delta t_{or} + \Delta t_{de} + \Delta t_{ac})_7$ OODA₇
Δt_v
$(\Delta t_{ob}+ \Delta t_{or} + \Delta t_{de} + \Delta t_{ac})_8$ OODA₈
Δt_f
$(\Delta t_{ob}+ \Delta t_{or} + \Delta t_{de} + \Delta t_{ac})_9$
t_0
t_{final}

$\Delta t_d = t_d - t_0$

$\Delta t_{ooda1} = t_{ooda1} - t_d$

$\Delta t_c = t_c - t_{de}$

$\Delta t_{ooda2} = t_{ooda2} - t_e$

$\Delta t_n = t_n - t_d$

$\Delta t_t = t_t - t_n$

$\Delta t_{ooda3} = t_{ooda3} - t_e$

$\Delta t_e = t_e - t_{ac}$

$\Delta t_{ooda4} = t_{ooda4} - t_e$

$\Delta t_i = t_i - t_{ooda4}$

$\Delta t_{ooda5} = t_{ooda5} - t_i$

$\Delta t_r = t_r - t_{ooda5}$

$\Delta t_{ooda6} = t_{ooda6} - t_r$

$\Delta t_{RCA} = t_{RCA} - t_{ooda6}$

$\Delta t_{ooda7} = t_{ooda7} - t_{RCA}$

$\Delta t_v = t_v - t_{ooda7}$

$\Delta t_{ooda8} = t_{ooda8} - t_v$

$\Delta t_f = t_f - t_{ooda8}$

$\Delta t_{ooda9} = t_{ooda9} - t_v$

t_0 is <u>initiation</u> of indicator
t_d is <u>initiation</u> of detection process
Δt_d is <u>duration</u> of detection process
t_{ooda2} is <u>initiation</u> of OODA process
Δt_{ooda2} is <u>duration</u> of OODA process
t_n is <u>initiation</u> of characterize process
Δt_n is <u>duration</u> of characterize process
t_{ooda2} is <u>initiation</u> of OODA process
Δt_{ooda2} is <u>duration</u> of OODA process
t_n is <u>initiation</u> of notify process
Δt_n is <u>duration</u> of notify process
t_t is <u>initiation</u> of triage process
Δt_t is <u>duration</u> of triage process
t_{ooda3} is <u>initiation</u> of OODA process
Δt_{ooda3} is <u>duration</u> of OODA process
t_e is <u>initiation</u> of escalate process
Δt_e is <u>duration</u> of escalate process
t_{ooda4} is <u>initiation</u> of OODA process
Δt_{ooda4} is <u>duration</u> of OODA process
t_i is <u>initiation</u> of isolate process
Δt_i is <u>duration</u> of isolate process
t_{ooda5} is <u>initiation</u> of OODA process
Δt_{ooda5} is <u>duration</u> of OODA process
t_r is <u>initiation</u> of restore process
Δt_r is <u>duration</u> of restore process
t_{ooda5} is <u>initiation</u> of OODA process
Δt_{ooda5} is <u>duration</u> of OODA process
t_{RCA} is <u>initiation</u> of root cause analysis (RCA) process
Δt_{RCA} is <u>duration</u> of RCA process
t_{ooda7} is <u>initiation</u> of OODA process
Δt_{ooda7} is <u>duration</u> of OODA process
t_v is <u>initiation</u> of recover process
Δt_v is <u>duration</u> of recover process
t_{ooda8} is <u>initiation</u> of OODA process
Δt_{ooda8} is <u>duration</u> of OODA process
t_f is <u>initiation</u> of feedback process
Δt_f is <u>duration</u> of feedback process
t_{ooda9} is <u>initiation</u> of OODA process
Δt_{ooda9} is <u>duration</u> of OODA process

t_0 Note: t_0 may not be known until after the fact

$t_{respond} = t_{final} - t_0$ <u>or</u> $t_{respond} = \text{å} \ (\Delta t_d, \Delta t_n, \Delta t_t, \Delta t_e, \Delta t_i, \Delta t_r, \Delta t_{RCA}, \Delta t_v, \Delta t_f) + \text{å} \ (\Delta t_{oooda1} \ldots \Delta t_{oooda9})$

26th annual INCOSE international symposium
Edinburgh, UK
July 18 - 21, 2016

OODA:

- Observe
- Orient
- Decide
- Act

SDM Structure

- For each of the 11 workflow phases:
  - – Capture anomaly processing time and quantity
- Distinguish *manual* v. *machine* processing
- Case study
  - – Knowledge encoding (*cybersecurity decision patterns*)
    - <u>Local</u> & <u>systemic</u> role, fit, function, and effects

PDF Determination Process

Determine *probability distribution functions* (PDFs)

- Anomaly processing scale
- Root in reality
- Ranges of data
- Specific data within ranges
- Goodness of fit
- Baseline v. estimated post-solution effects

Anomaly Processing Scale[1]

# Minutes	Label	Description
1	seconds	less than a minute (<60 sec)
60	minutes	less than an hour (<60 min)
1440	hours	less than a day (<24 hours)
10080	days	less than a week (<7 days)
40320	weeks	less than a month (<4 weeks)
483840	months	less than a year (<12 months)
1051200	years	up to 2 years (<2 years)

[1] Derived from Ponemon 2014 Data Breach Report

Example PDF Table for Manual Detect

P(x)	Cum(x)	Time (minutes)
0	0	1
0.122	0.122	60
0.256	0.378	1440
0.322	0.7	10080
0.178	0.878	40320
0.089	0.967	483840
0.033	1	1051200

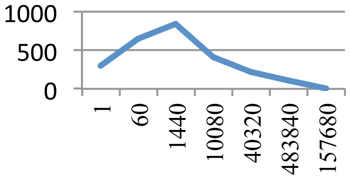
PDF Application

Generate data points w/ basis in reality

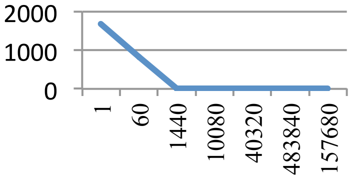
- Use Excel
- 5,000 data points per workflow phase
  - Generate random numbers
  - Use VLOOKUP on probability distribution scale
  - 5,000 anomaly processing *time ranges* per phase

Probability Distribution Graphs

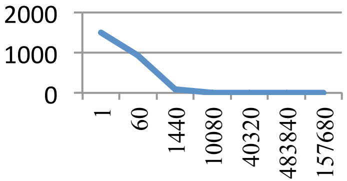
Detect



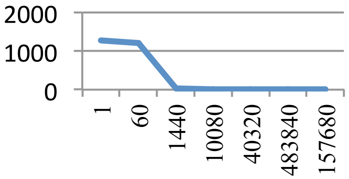
Characterize



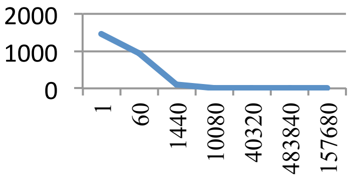
Notify



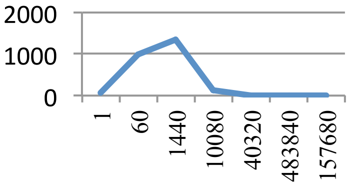
Triage



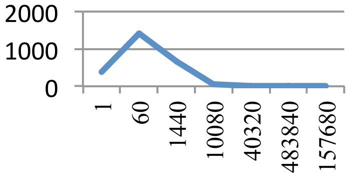
Escalate



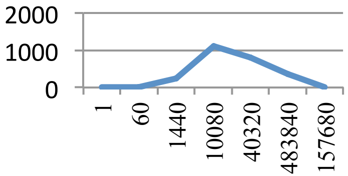
Isolate



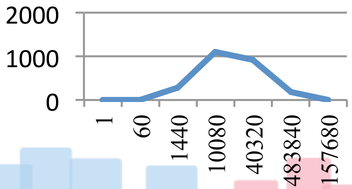
Restore



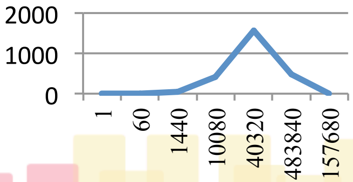
RCA



Recover



Feedback



Baseline PDFs for the SDM

Phase	Pre-<proposed solution> PDFs	
	Manual	Machine
Detect	WEIBULL(.33264,1869,922)	LOGNORMAL(41961.42,58278966.6,923)
Characterize	LOGNORMAL(20,280,924)	LOGNORMAL(1.68,5.14,925)
Notify	LOGNORMAL(40,751,109)	LOGNORMAL(2.33,9.1,110)
Triage	LOGNORMAL(53,920,227)	LOGNORMAL(2.59,10.73,228)
Escalate	LOGNORMAL(53,1252,228)	LOGNORMAL(3.06,14.77,229)
Isolate	WEIBULL(.56032,432,112)	LOGNORMAL(468.59,21153.18,113)
Restore	LOGNORMAL(1117,35405,1962)	LOGNORMAL(108.72,4431.36,1963)
RCA	UNIFORM(41, 483856,1938)	NA
Recover	UNIFORM(41, 483714,1966)	UNIFORM(0, 482793,1967)
Feedback	UNIFORM(43, 483621,1935)	NA

Estimating Solution Effects

- Effects reflected in PDF tables
  - One or more workflow phases
    - May be uniform across relevant phases
    - May vary across relevant phases
- New probability distribution functions (PDFs)
- Modify SDM with new PDFs
- Rerun SDM
- Compare post-solution results to baseline

PDFs for Estimated Improvements

Phase	Post-CDPs (1% improvement) Manual	Post-CDPs (2.5% improvement) Manual	Post-CDPs (5% improvement) Manual	Post-CDPs (10% improvement) Manual
Detect	LOGNORMAL(143551.89,82229861.89, 922)	LOGNORMAL(138023.37,78478463.84, 922)	LOGNORMAL(154200.65,104251444.55, 922)	LOGNORMAL(148223.09,107706259.16, 922)
Characterize	LOGNORMAL(19.68,264.5,924)	LOGNORMAL(18.27,237.19,924)	LOGNORMAL(18.24,243.6,924)	LOGNORMAL(16.35,204,924)
Notify	LOGNORMAL(39.73,743.74,109)	LOGNORMAL(37.73,699.41,109)	LOGNORMAL(35.17,622.00,109)	LOGNORMAL(32.59,574.06,109)
Triage	LOGNORMAL(50.50,841.15,227)	LOGNORMAL(51.01,864.12,227)	LOGNORMAL(45.39,734.13,227)	LOGNORMAL(42.55,701.07,227)
Escalate	LOGNORMAL(53.02,1249.91,228)	LOGNORMAL(49.89,1144.86,228)	LOGNORMAL(48.45,1104.96,228)	LOGNORMAL(40.34,843.40,228)
Isolate	WEIBULL(.55865,417.92,112)	GAMMA(.42373,1642.36,112)	WEIBULL(.54394,389.6,112)	GAMMA(.38757,1672.44,112)
Restore	LOGNORMAL(1107.69,35920.96,1962)	LOGNORMAL(1131.34,39243.71,1962)	LOGNORMAL(1231.24,50136.44,1962)	LOGNORMAL(1134.13,50499.44,1962)
RCA	UNIFORM(0,483512,1938)	UNIFORM(0,483840,1938)	UNIFORM(0,483700,1938)	UNIFORM(0,483797,1938)
Recover	UNIFORM(0,483858,1966)	UNIFORM(0,483854,1966)	UNIFORM(0,483798,1966)	UNIFORM(0,483802,1966)
Feedback	UNIFORM(0,483815,1935)	UNIFORM(0,483857,1935)	UNIFORM(0,483859,1935)	UNIFORM(0,483787,1935)

Results Analysis

Quantity

- All anomaly processing quantities went up (incr efficiency)
  - Expected due to effect assumptions

Time

- Some anomaly processing times went down (incr efficiency)
- Some went up (decr efficiency)

∴ Quantity increase shifted bottlenecks down stream

∴ More anomalies are in phases that take longer to process, thus increasing mean times

Conclusions

- Consummate systems thinking challenge
  - Behavior within the whole
  - Behavior of the whole
  - Conceptualize local changes in context of the whole
- Improving cybersecurity operations
  - A multi-step, multi-year process
  - Shifting future focus according to current results
- Model helps anticipate effects
  - Validate expected consequences
  - Identify unanticipated consequences

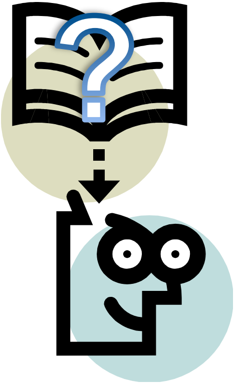
Future

- Run model for multiple years
- Dynamic feedback of CDP (knowledge) production
  - Manual anomaly processing
  - Machine anomaly processing
    - Knowledge effects on machine processing
- Upper bounds to improvements
- Add knowledge degradation
- Monetize model
  - Associate dollars to anomaly processing time
  - ROI decision support
- Model verification and validation

Future continued…

- Causal loop feedbacks:
  - To Perimeter Defense effectiveness from RCA
- Distinguish types of anomalies
- Distinguish anomaly impact (for cost estimates)
- Distinguish type of manual resource
  - Novice, journeyman, master, subject matter expert (varying costs)
- Model shift in processing from SME to novice over time

Questions



Backup Slides

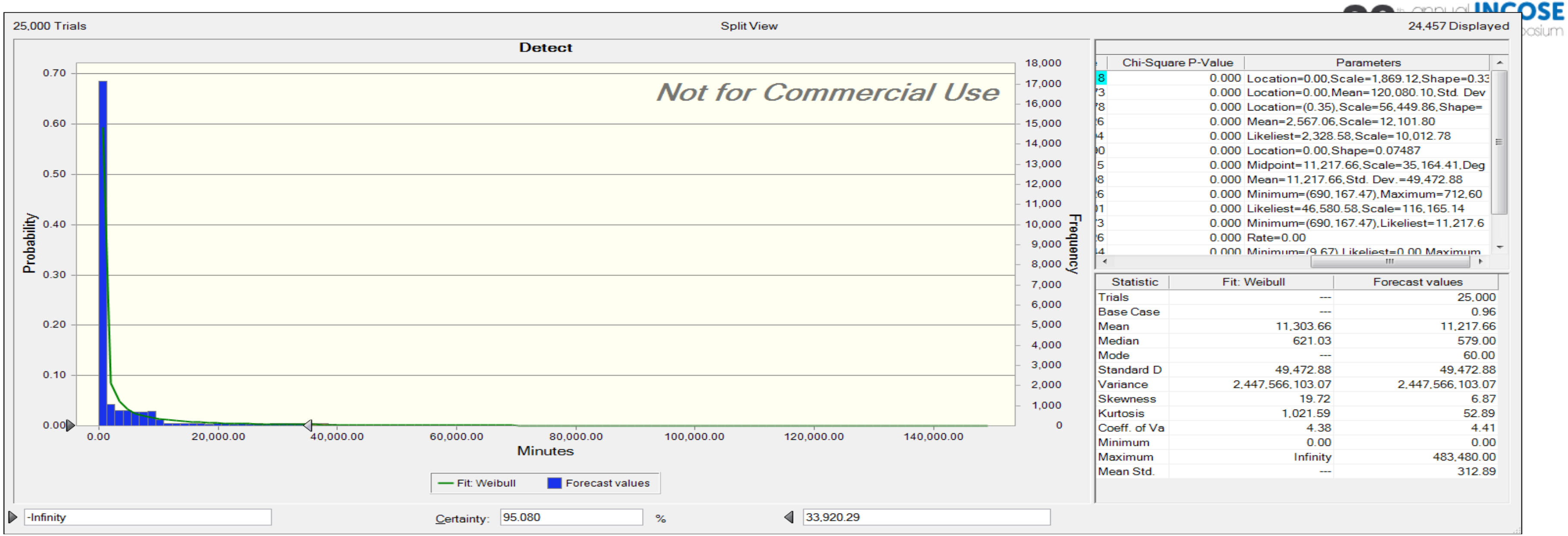
26th annual INCOSE international symposium

Edinburgh, UK
July 18 - 21, 2016

Probability Distribution Ranges Excerpt

r(Det)	Detect (MTTD)	r(Char)	Characterize (MTTC)	r(Not)	Notify (MTTN)	r(Tri)	Triage (MTTT)
0.12539634	60	0.99450602	1440	0.50902739	1	0.82893511	60
0.83770346	10080	0.76424075	60	0.02691813	1	0.38211664	1
0.55457905	1440	0.55108253	1	0.50498849	1	0.85421571	60
0.98757692	483840	0.5296778	1	0.12907582	1	0.48586495	1

Goodness of Fit Test Example: MTTD Manual



	Chi-Square P-Value	Parameters
8	0.000	Location=0.00,Scale=1,869.12,Shape=0.33
73	0.000	Location=0.00,Mean=120,080.10,Std. Dev
78	0.000	Location=(0.35),Scale=56,449.86,Shape=
6	0.000	Mean=2,567.06,Scale=12,101.80
4	0.000	Likeliest=2,328.58,Scale=10,012.78
0	0.000	Location=0.00,Shape=0.07487
5	0.000	Midpoint=11,217.66,Scale=35,164.41,Deg
8	0.000	Mean=11,217.66,Std. Dev.=49,472.88
6	0.000	Minimum=(690,167.47),Maximum=712,60
1	0.000	Likeliest=46,580.58,Scale=116,165.14
3	0.000	Minimum=(690,167.47),Likeliest=11,217.6
6	0.000	Rate=0.00
4	0.000	Minimum=(9.67),Likeliest=0.00,Maximum

Statistic	Fit: Weibull	Forecast values
Trials	---	25,000
Base Case	---	0.96
Mean	11,303.66	11,217.66
Median	621.03	579.00
Mode	---	60.00
Standard D	49,472.88	49,472.88
Variance	2,447,566,103.07	2,447,566,103.07
Skewness	19.72	6.87
Kurtosis	1,021.59	52.89
Coeff. of Va	4.38	4.41
Minimum	0.00	0.00
Maximum	Infinity	483,480.00
Mean Std.	---	312.89

Results (Quantity)

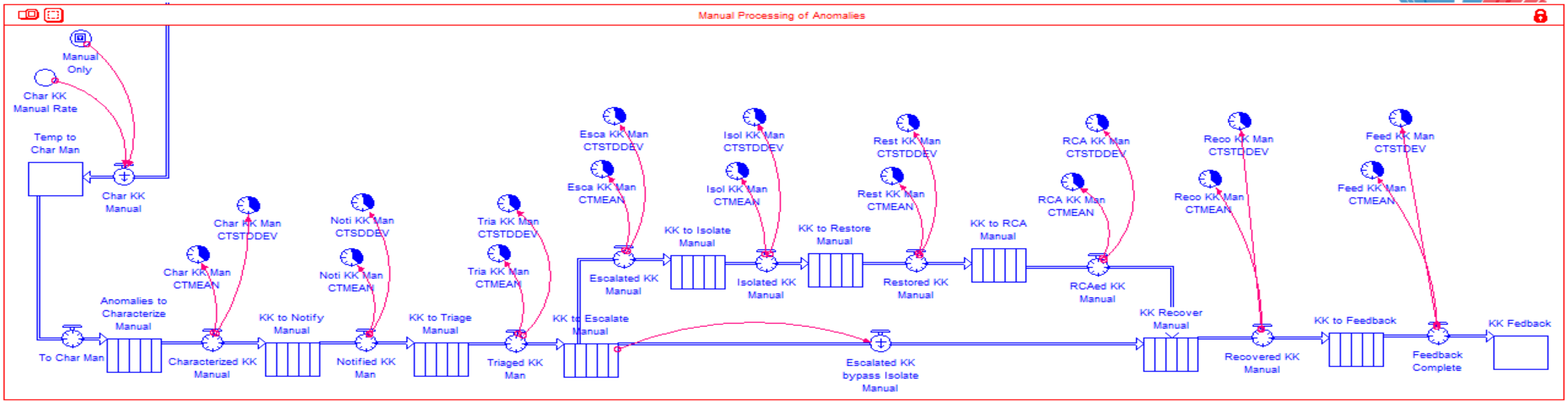
Run	KK Characterized Man Total	KK Notified Man Total	KK Triaged Man Total	KK Escalated Man Total	KK Isolated Man Total	KK Restored Man Total	KK RCAed Man Total
Base	1,398.30	1,398.13	1,397.93	1,397.64	172.24	171.90	90.65
1.00%	1,473.80	1,473.74	1,473.66	1,473.58	179.24	178.94	95.01
2.50%	1,444.26	1,444.15	1,443.94	1,443.70	175.90	175.36	96.95
5.00%	1,511.24	1,511.02	1,510.81	1,510.48	185.95	185.62	99.45
10.00%	1,776.47	1,776.35	1,776.18	1,775.88	217.65	217.25	117.79

Results (Time)

Run	Char KK Man	Noti KK Man	Tria KK Man	Esca KK Man	Isol KK Man	Rest KK Man	RCA KK Man	Reco KK Man	Feed KK Man
Base	20.46	36.59	50.61	47.12	691.09	835.41	167,908.13	169,164.61	130,950.15
1.00%	19.39	35.74	48.75	41.61	659.48	710.03	169,752.36	172,402.66	130,105.57
2.50%	19.80	35.07	47.92	66.93	700.82	836.99	168,163.12	170,674.75	129,303.08
5.00%	18.92	33.36	41.24	48.92	703.79	767.87	174,788.95	171,261.98	130,862.45
10.00%	16.04	31.07	42.20	39.58	655.98	852.81	170,105.83	171,888.20	132,641.70

Run	Char KK Man	Noti KK Man	Tria KK Man	Esca KK Man	Isol KK Man	Rest KK Man	RCA KK Man	Reco KK Man	Feed KK Man
Base									
1.00%	5.22%	2.34%	3.68%	11.69%	4.57%	15.01%	-1.10%	-1.91%	0.64%
2.50%	3.25%	4.16%	5.32%	-42.03%	-1.41%	-0.19%	-0.15%	-0.89%	1.26%
5.00%	7.55%	8.83%	18.52%	-3.81%	-1.84%	8.09%	-4.10%	-1.24%	0.07%
10.00%	21.59%	15.09%	16.62%	15.99%	5.08%	-2.08%	-1.31%	-1.61%	-1.29%

SDM Excerpt


Manual Processing of Anomalies
Manual Only
Char KK Manual Rate
Temp to Char Man
Char KK Manual
Char KK Man CTSTDDEV
Char KK Man CTMEAN
Anomalies to Characterize Manual
To Char Man
Characterized KK Manual
KK to Notify Manual
Noti KK Man CTSDDEV
Noti KK Man CTMEAN
Notified KK Man
KK to Triage Manual
Tria KK Man CTSTDDEV
Tria KK Man CTMEAN
Triaged KK Man
KK to Escalate Manual
Esca KK Man CTSTDDEV
Esca KK Man CTMEAN
Escalated KK Manual
KK to Isolate Manual
Isol KK Man CTSTDDEV
Isol KK Man CTMEAN
Isolated KK Manual
KK to Restore Manual
Rest KK Man CTSTDDEV
Rest KK Man CTMEAN
Restored KK Manual
KK to RCA Manual
RCA KK Man CTSTDDEV
RCA KK Man CTMEAN
RCAed KK Manual
Escalated KK bypass Isolate Manual
KK Recover Manual
Reco KK Man CTSTDDEV
Reco KK Man CTMEAN
Recovered KK Manual
KK to Feedback
Feed KK Man CTSTDEV
Feed KK Man CTMEAN
Feedback Complete
KK Fedback