Applying CMMI to System Safety

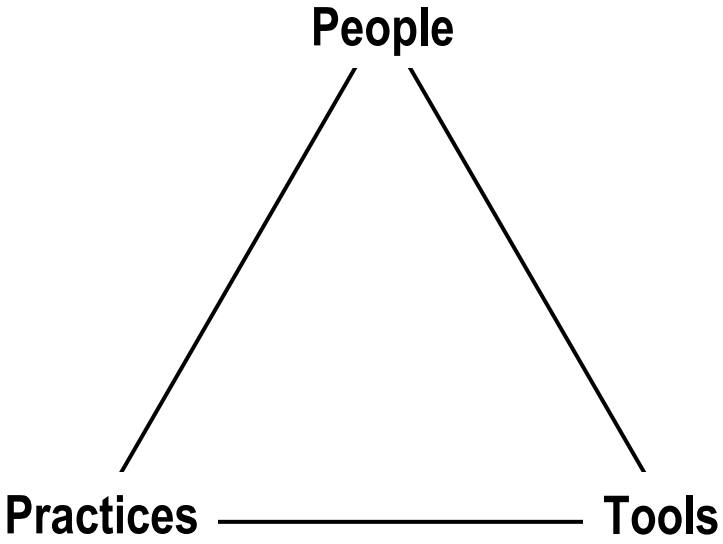
APT Research, Inc.

Tom Pfitzer

A-P-T Research, Inc.

Good System Safety Programs

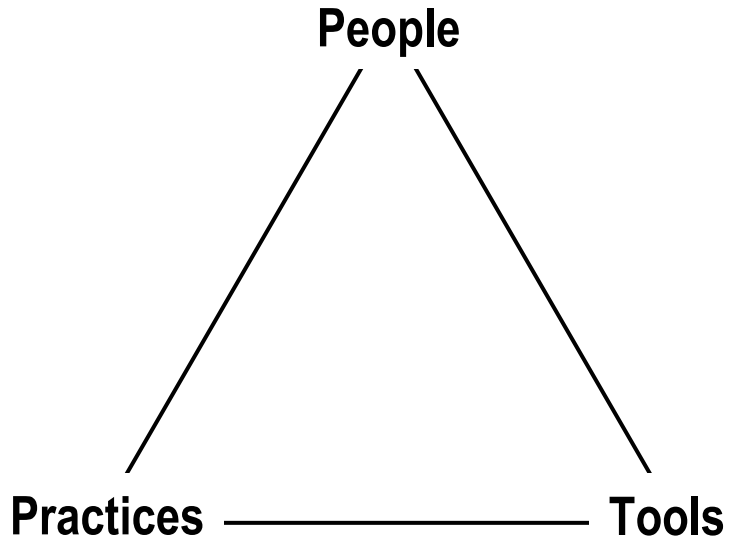
A combination of factors related to people, practices and tools result in the goodness of a system safety program



Each of the main factors can be evaluated to predict the adequacy of the resulting safety program

The CMM Concept

The maturity of an organization's capability depend upon 3 interrelated elements



Maturity is measured by

Achievement Levels:

0 – Incomplete/Entry-level or repeated fledgling level analyses, casually performed

1 – Pro forma/Perfunctorily

2 – Managed (work guided and overseen by trained Supv.)

3 – Defined

4 – Quantified (Metrics applied to various determinants/discriminants)

5 – Optimized (Superior)

Why CMM?

Capability Maturity Model Integration

"…the quality of a system or product is highly influenced by the quality of the process used to develop and maintain it."

Mary Beth Chrissis, et al

"You take you car into a lousy shop, you're gonna get a lousy job!"

Tom & Ray Magliazi

The Use of the CMMI approach could provide:

A. Government organizations a means to specify or evaluate industry safety programs
B. Mature industry and government programs a means to "certify" existing maturity
C. Immature industry or Government programs a way ahead toward more maturity

A-P-T Research, Inc.

The CMMI Approach to any discipline such as System Safety

	Personnel			Methods			Tools		
	P_1	P_2	P_3…	M_1	M_2	M_3…	T_1	T_2	T_3…
0 - Incomplete	None	None	None	None	None	None	None	None	None
1 – Performed	x	y	z	a	b	c	q	r	s
2 – Managed	xx	yy	zz	aa				rr	ss
3 – Defined	xxx	yyy	zzz			ccc	qqq	rrr	sss
4 – Quantitatively Managed	xxxx	yyyy	zzzz	aaaa	bbbb	cccc	qqqq	rrrr	ssss
5 - Optimized	xxxxx	yyyyy	zzzzz	aaaaa	bbbbb	ccccc	qqqqq	rrrrr	sssss

Notional

Measurement Categories

Measurement Indices

Levels of Maturity

Personnel

	P_1 - Training	P_2 - Experience	P_3 - Credentials	P_4 - Depth of Staff	P_5 …
0	None	None		0 - 1 Fulltime	
1	1 Week Training	1 – 3 Years			
2	3 – 5 Short Courses	3 – 7 Years	SSS Mer		
3		7 – 15			
4		15 – 25 Years			
5	Advanced Degree in System Safety	25 + Years	Advanced Degree		

Notional

Methods

	M_1 – Review of Analysis	M_2 – Matrix Tailoring	M_3 – Mission Phasing	M_4 – Asset Selection	M_5 – Use Effectiveness Hierarchy	M_6 – Use of Risk Tolerant Limits	M_7 – Hazard Tracking
0							
1	None performed (solo Analysis)	None performed	None	Pro-forma (ad-hoc)	Not evident		None
2	Peer (1)	Disciplined matrix selection	Modest, pro-forma (eg., startup/run/stop)	Two, rote-selected	Used but not monitored		Informal
3	Peer/Mgmnt (>1 or 1st level mgmnt)	Subjective matrix tailoring	TRR, [illegible] selected		Used and Monitored		Procedure-driven, documented
4	Mgmnt (2nd level)	Quantitative matrix scaling	All significant transients	3, + severity levels tailored to case	Use enforced		Coupled w/Config. Mgmnt. or Quality Prgm
5	3rd Party (>5 long-term sample)	Full Matrix (indicates/spans /Resolution)	4, + maintenance/ calibration, etc.	3 & 4, + maintenance/ calibration, etc.	4, + design change use generously evident		4, + auditable evidence of closeout

A-P-T Research, Inc.

Methods (cont.)

	M_8 – Influence of Design	M_9 – Cross Coupled "illities"	M_{10} – Selection of Risk Tolerant Limits	M_{11} – Risk Summation	M_{12} – Hazard Identification
0					
1	None	None	Pro-forma	None	"What-if"
2	Infrequent design reviews (e.g., 30/60/90%)	Modest, informal cross-feed w/Reliability	TBD	Subjective, loosely disciplined	1, + Checklist
3	Frequent design reviews (e.g., ≈15% intervals)	Formal, mandatory cross-feed w/Reliability	TBD	Procedurally documented	2, + Energy source inventory
4	Concurrent engineering	TBD	TBD	3, + Numerically done	Operational walkthroughs
5	Designers trained/intermediate application	Full-bore, readily auditable w/Reliability, Availability	Tailored to program/system needs	Rigorous	3 &4, + FMEA or HAZOP, or FHA

Tools

	T_1 – Hazard Inventory Tools	T_2 – Logic Tree Tools	T_3 – Probalistic Risk Assessment
0			
1	PHL	FTA (unquantified)	TBD
2	PHA (w/o matrix use)	ETA (unquantified)	TBD
3	PHA or HAZOP (w/matrix)	FTA a/o ETA (quantified)	TBD
4	FMEA or FHA	CCA (quantified)	TBD
5	Top-Down + Bottom-Up	CCA + (FTA or ETA)	TBD

Conclusion

- If interest exists, G-48 could develop recommended standards to measure/evaluate System Safety program maturity.
  - APT will host a collegial workshop to define a strawman set of measurement categories and indices for each.
  - Produce a report with recommended categories and indices.

Contact Information:

Tom Pfitzer

256.327.3388

A-P-T Research, Inc.

pfitzer@apt-research.com