Space Shuttle Program
Primary Avionics Software System (PASS)
Success Legacy – Quality & Reliability Date

James K. Orr

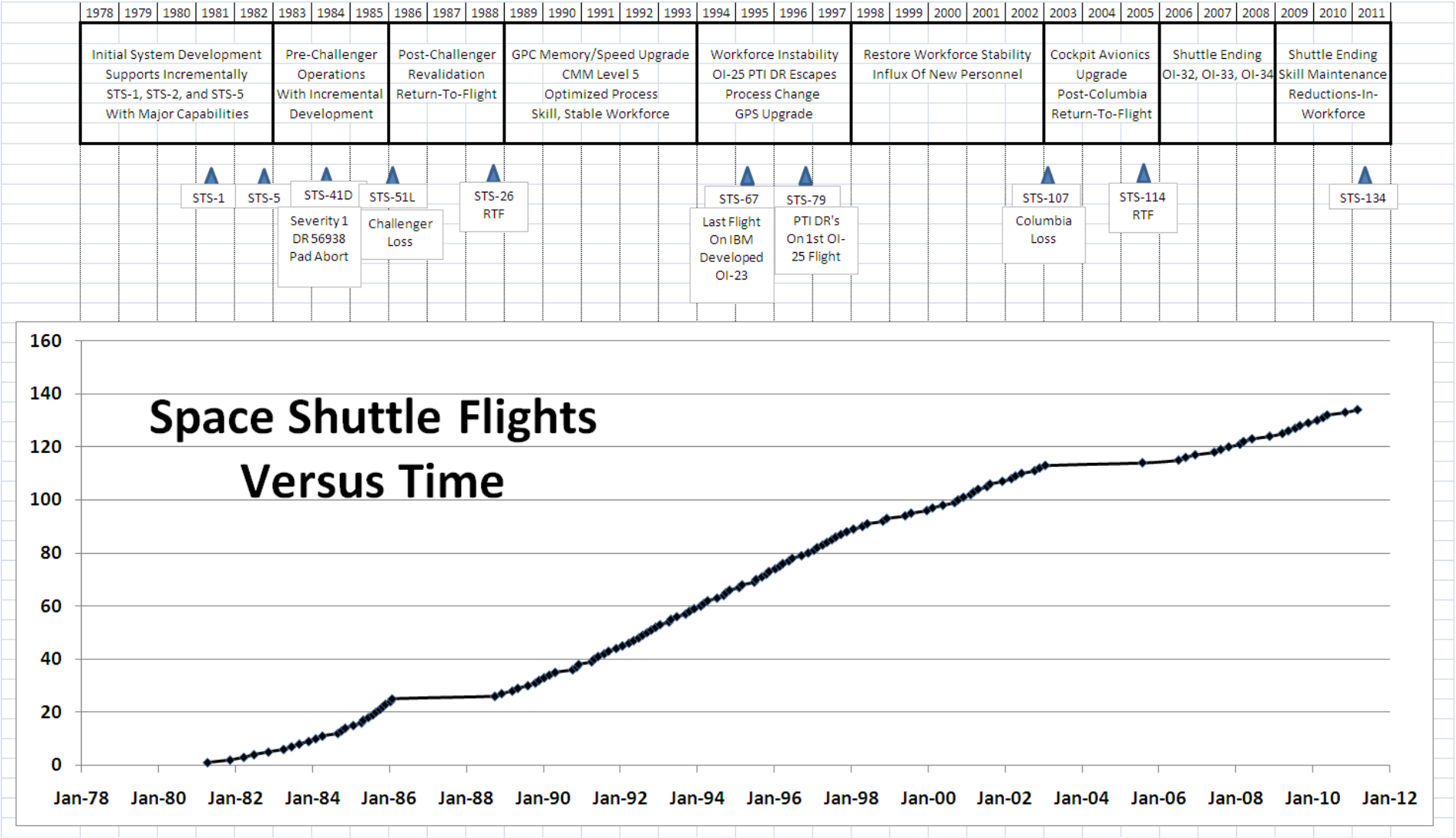
August 24, 2010

United Space Alliance

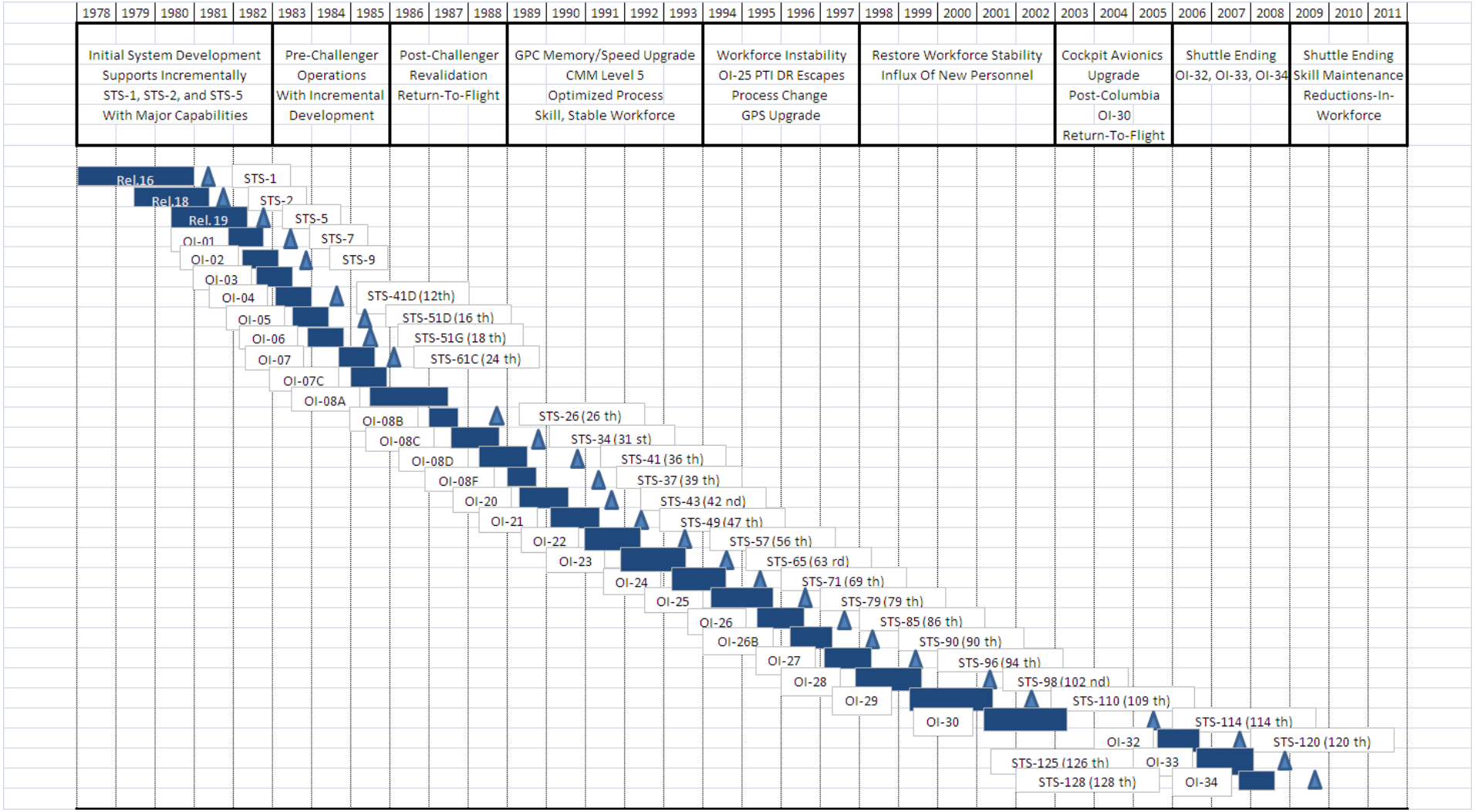
PASS Project Overview

- Project and process evolution began in mid-70's
- Software exhibits world-class quality and reliability for life-critical operations
  - Very high maturity software process (NASA HQ assessed as SEI Level 5)
  - ISO 9001 registered process
  - 29 + years of demonstrated flight safety and ultra-reliability
  - CMMI Level 5 in 2006, 2009
- Onboard software controls all phases of Shuttle flights (manual and auto)
- Primary Avionics Software System (PASS)
  - Provides automatic and fly-by-wire control of critical shuttle systems which executes in redundant computers
  - 450,000 SLOC primarily in HAL/S
    - Total lines have remained relatively constant over the multiple releases since STS-5

Key Space Shuttle Flight

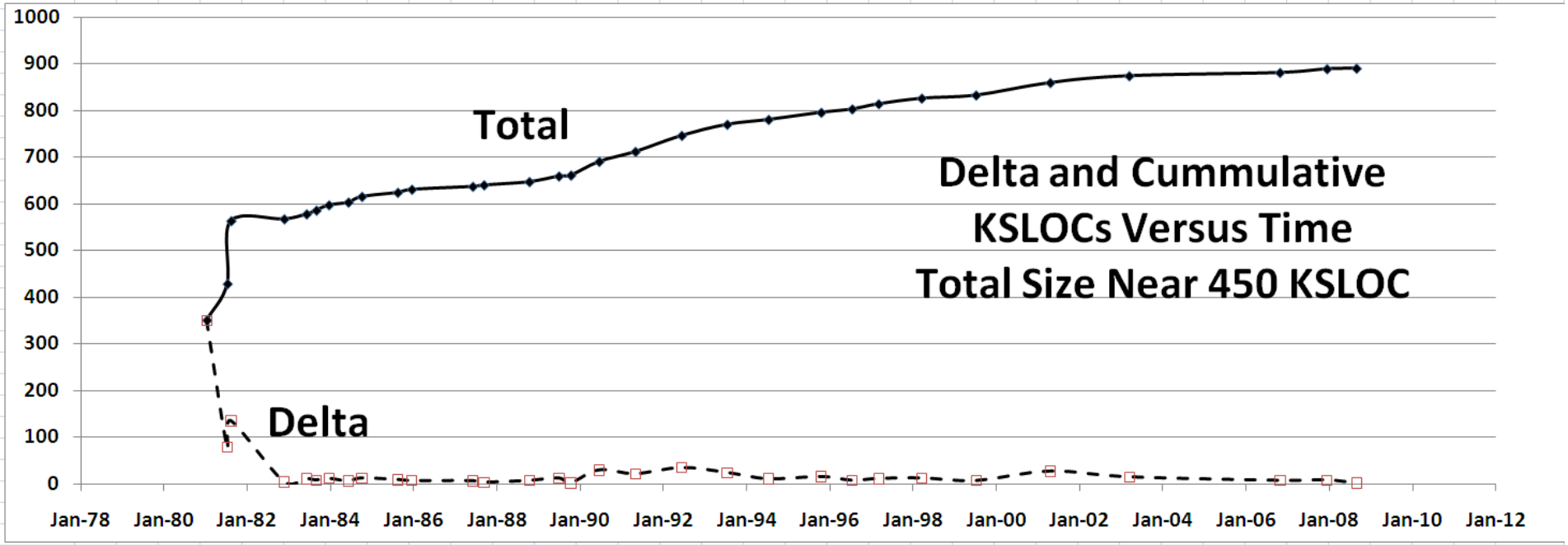


PASS FSW Development History



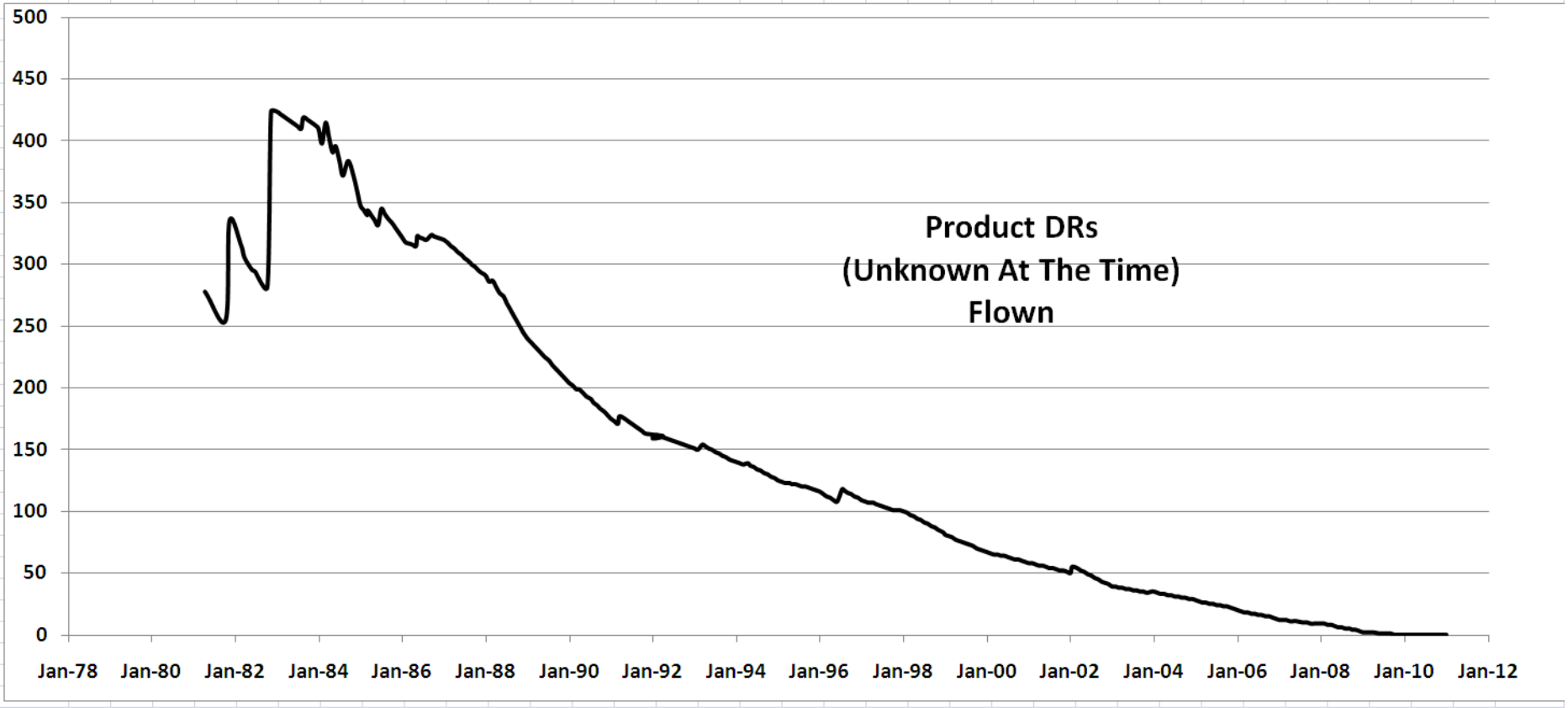
PASS FSW Incremental Change Size

1978	1979	1980	1981	1982	1983	1984	1985	1986	1987	1988	1989	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011
Initial System Development Supports Incrementally STS-1, STS-2, and STS-5 With Major Capabilities					Pre-Challenger Operations With Incremental Development			Post-Challenger Revalidation Return-To-Flight			GPC Memory/Speed Upgrade CMM Level 5 Optimized Process Skill, Stable Workforce					Workforce Instability OI-25 PTI DR Escapes Process Change GPS Upgrade					Restore Workforce Stability Influx Of New Personnel					Cockpit Avionics Upgrade Post-Columbia Return-To-Flight			Shuttle Ending OI-32, OI-33, OI-34			Shuttle Ending Skill Maintenance Reductions-In-Workforce		



Number Of Latent Unknown Product DRs Flown

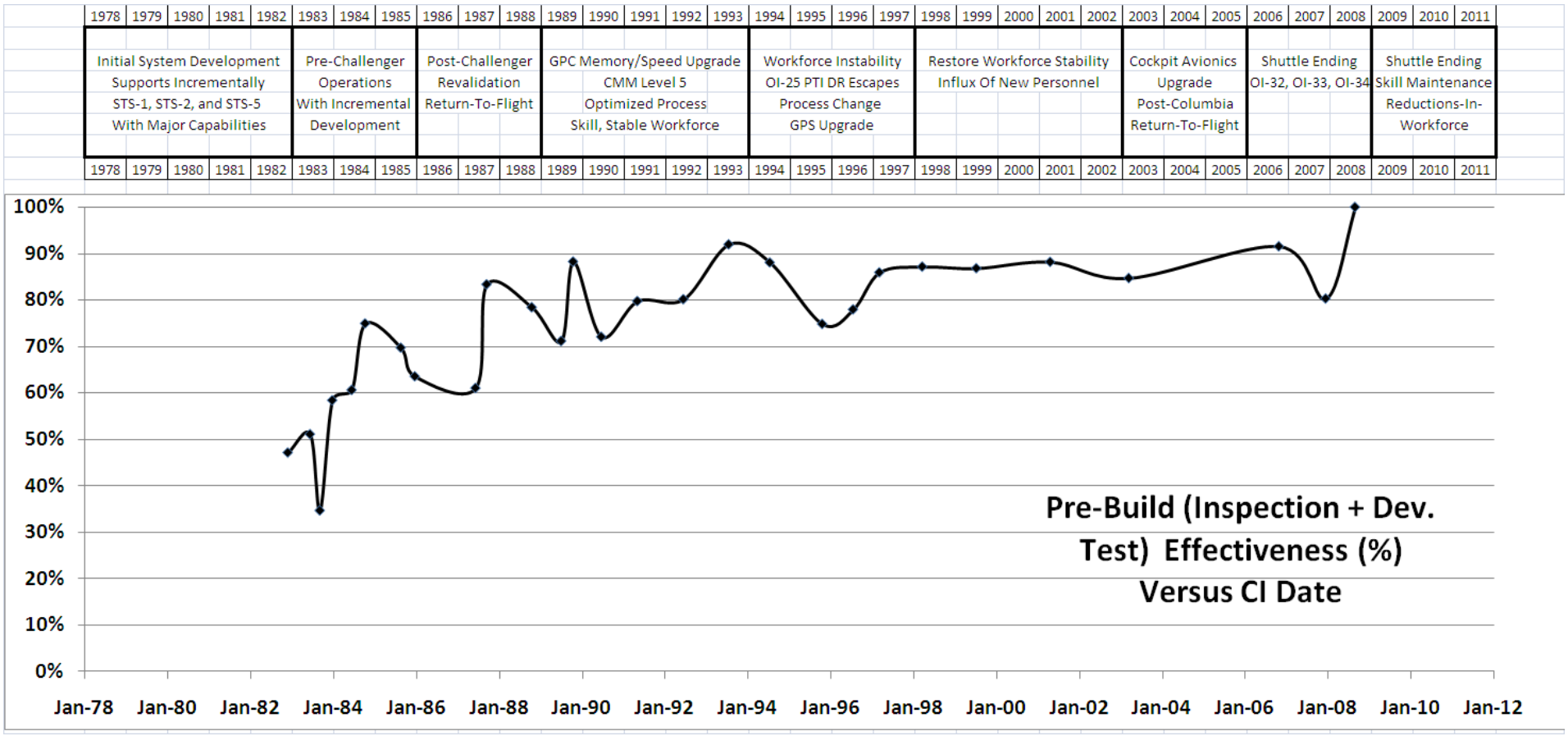
1978	1979	1980	1981	1982	1983	1984	1985	1986	1987	1988	1989	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011
Initial System Development Supports Incrementally STS-1, STS-2, and STS-5 With Major Capabilities					Pre-Challenger Operations With Incremental Development			Post-Challenger Revalidation Return-To-Flight			GPC Memory/Speed Upgrade CMM Level 5 Optimized Process Skill, Stable Workforce					Workforce Instability OI-25 PTI DR Escapes Process Change GPS Upgrade					Restore Workforce Stability Influx Of New Personnel					Cockpit Avionics Upgrade Post-Columbia Return-To-Flight			Shuttle Ending OI-32, OI-33, OI-34			Shuttle Ending Skill Maintenance Reductions-In-Workforce		
1978	1979	1980	1981	1982	1983	1984	1985	1986	1987	1988	1989	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011



Product DRs that existed on a flown system, but were unknown at the time of the flight . Discovered up to 25 years later.

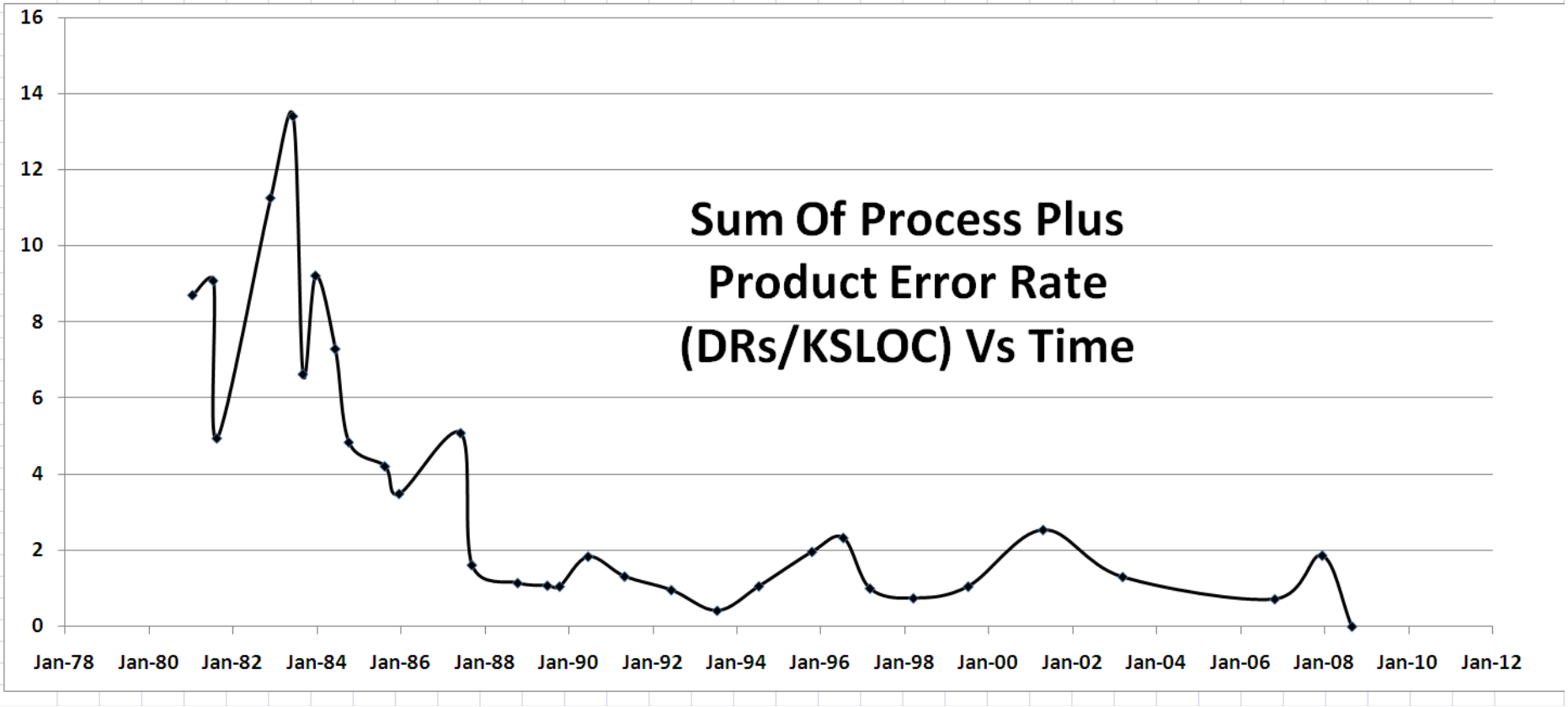
Pre-Build Error Removal

Effects Of Inspection and Pre-Build Testing



Post Build Error Rate (Process + Product)

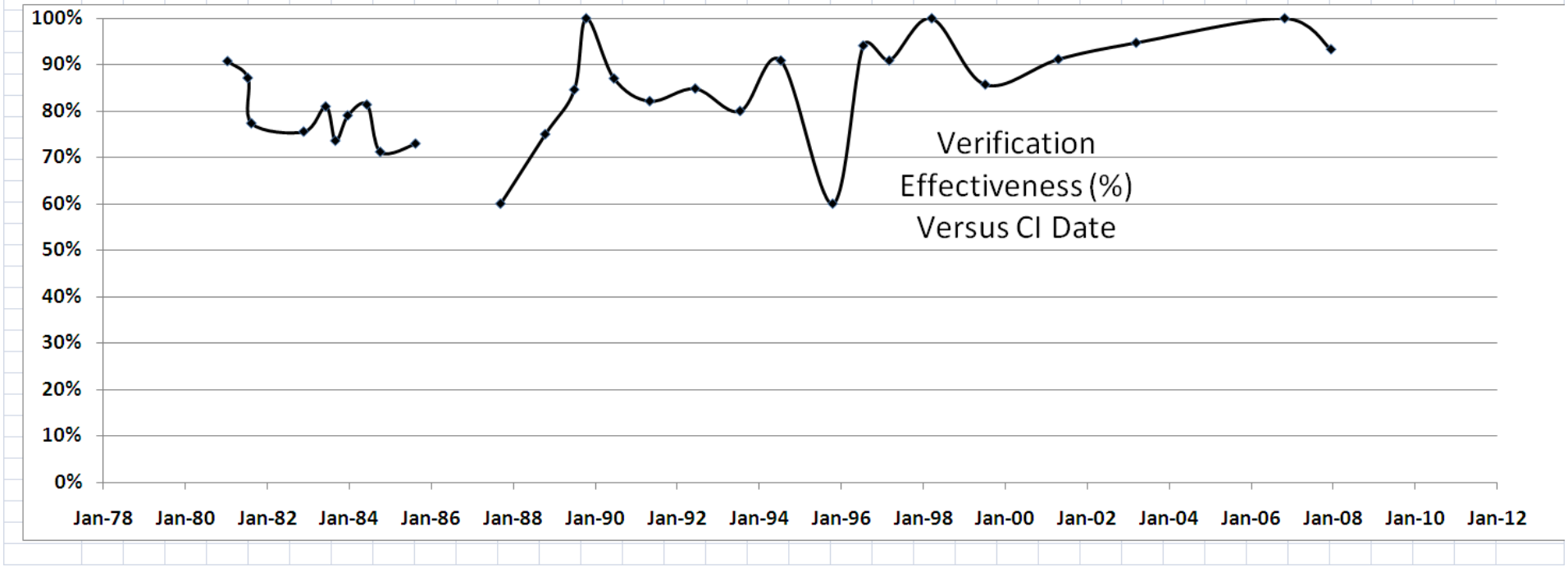
1978	1979	1980	1981	1982	1983	1984	1985	1986	1987	1988	1989	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011
Initial System Development Supports Incrementally STS-1, STS-2, and STS-5 With Major Capabilities					Pre-Challenger Operations With Incremental Development			Post-Challenger Revalidation Return-To-Flight			GPC Memory/Speed Upgrade CMM Level 5 Optimized Process Skill, Stable Workforce					Workforce Instability OI-25 PTI DR Escapes Process Change GPS Upgrade					Restore Workforce Stability Influx Of New Personnel					Cockpit Avionics Upgrade Post-Columbia Return-To-Flight			Shuttle Ending OI-32, OI-33, OI-34			Shuttle Ending Skill Maintenance Reductions-In-Workforce		
1978	1979	1980	1981	1982	1983	1984	1985	1986	1987	1988	1989	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011



Verification Effectiveness

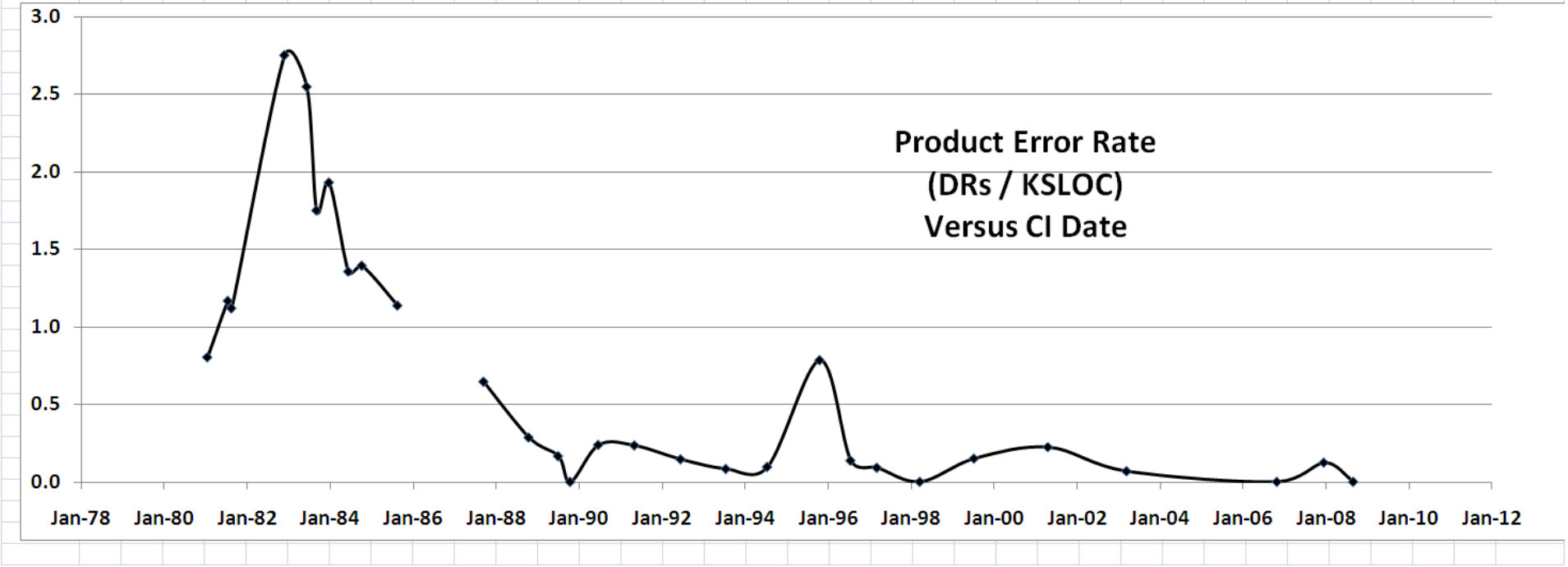
Process DRs / (Process + Product DRs)

1978	1979	1980	1981	1982	1983	1984	1985	1986	1987	1988	1989	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011
Initial System Development Supports Incrementally STS-1, STS-2, and STS-5 With Major Capabilities					Pre-Challenger Operations With Incremental Development			Post-Challenger Revalidation Return-To-Flight			GPC Memory/Speed Upgrade CMM Level 5 Optimized Process Skill, Stable Workforce					Workforce Instability OI-25 PTI DR Escapes Process Change GPS Upgrade					Restore Workforce Stability Influx Of New Personnel					Cockpit Avionics Upgrade Post-Columbia Return-To-Flight			Shuttle Ending OI-32, OI-33, OI-34			Shuttle Ending Skill Maintenance Reductions-In-Workforce		



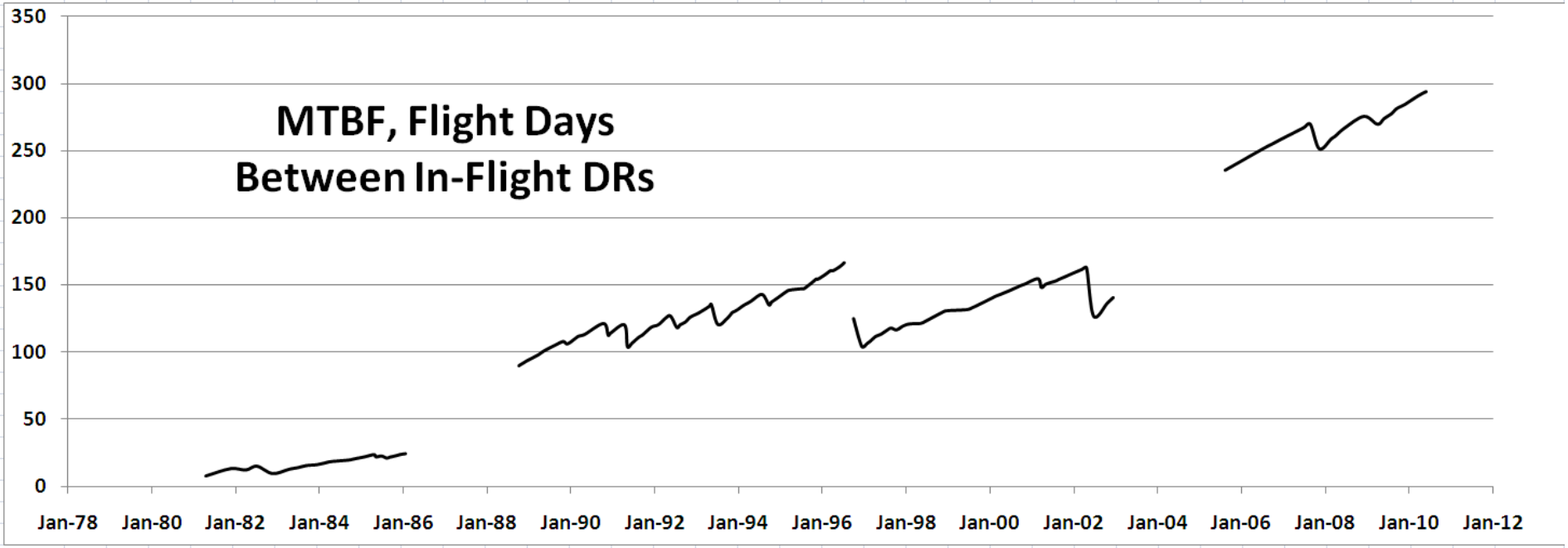
Product DR Rate

1978	1979	1980	1981	1982	1983	1984	1985	1986	1987	1988	1989	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011
Initial System Development Supports Incrementally STS-1, STS-2, and STS-5 With Major Capabilities					Pre-Challenger Operations With Incremental Development			Post-Challenger Revalidation Return-To-Flight			GPC Memory/Speed Upgrade CMM Level 5 Optimized Process Skill, Stable Workforce					Workforce Instability OI-25 PTI DR Escapes Process Change GPS Upgrade					Restore Workforce Stability Influx Of New Personnel					Cockpit Avionics Upgrade Post-Columbia Return-To-Flight			Shuttle Ending OI-32, OI-33, OI-34			Shuttle Ending Skill Maintenance Reductions-In-Workforce		
1978	1979	1980	1981	1982	1983	1984	1985	1986	1987	1988	1989	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011



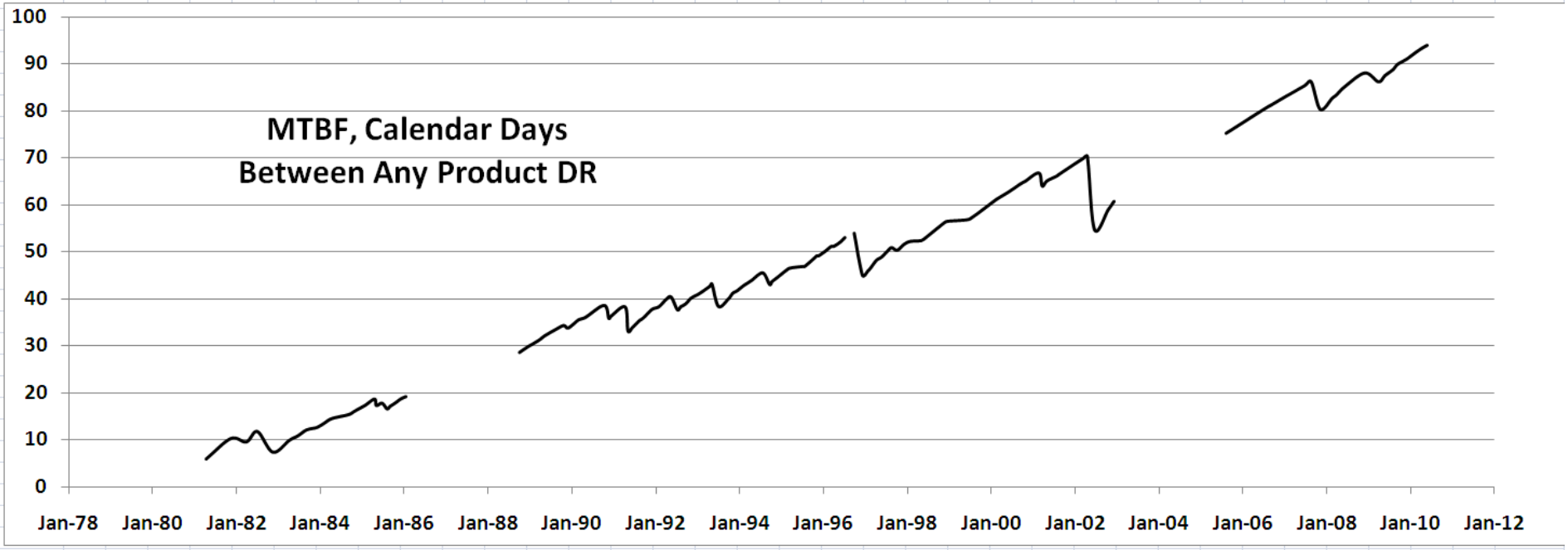
MTBF, Flight Days Between In-Flight DRs

1978	1979	1980	1981	1982	1983	1984	1985	1986	1987	1988	1989	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011
Initial System Development Supports Incrementally STS-1, STS-2, and STS-5 With Major Capabilities					Pre-Challenger Operations With Incremental Development			Post-Challenger Revalidation Return-To-Flight			GPC Memory/Speed Upgrade CMM Level 5 Optimized Process Skill, Stable Workforce					Workforce Instability OI-25 PTI DR Escapes Process Change GPS Upgrade					Restore Workforce Stability Influx Of New Personnel					Cockpit Avionics Upgrade Post-Columbia Return-To-Flight			Shuttle Ending OI-32, OI-33, OI-34			Shuttle Ending Skill Maintenance Reductions-In-Workforce		
1978	1979	1980	1981	1982	1983	1984	1985	1986	1987	1988	1989	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011



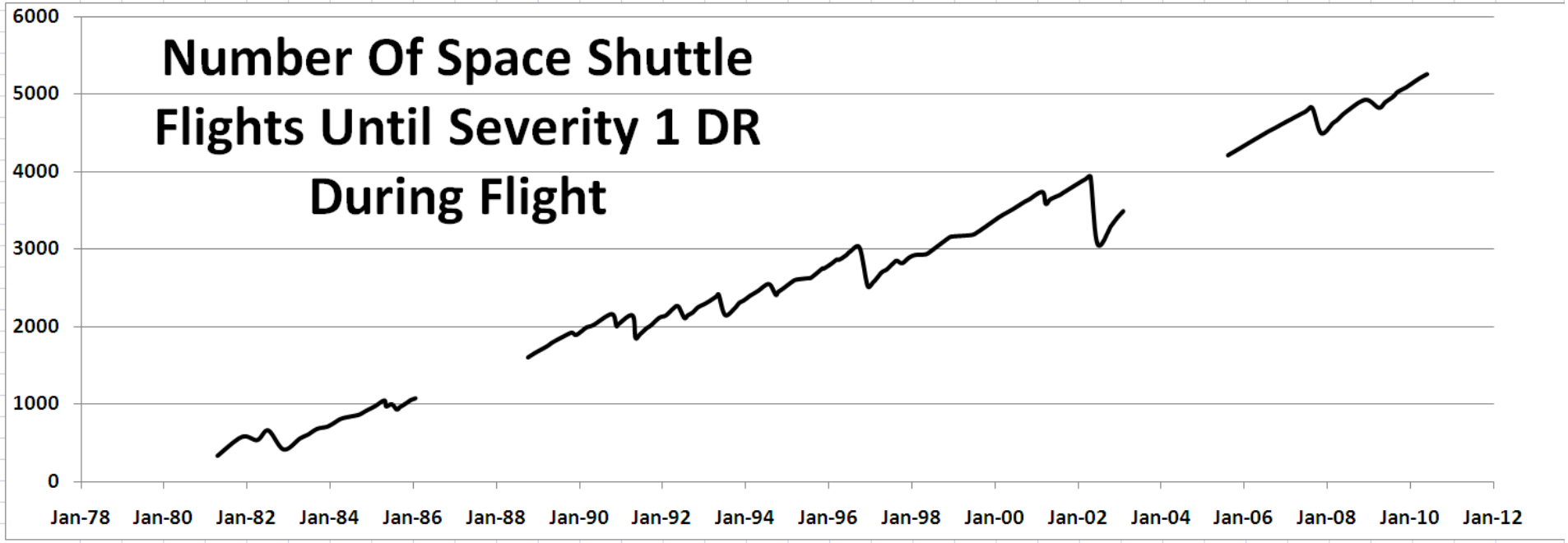
MTBF, Calendar Days Between Ground DRs

1978	1979	1980	1981	1982	1983	1984	1985	1986	1987	1988	1989	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011
Initial System Development Supports Incrementally STS-1, STS-2, and STS-5 With Major Capabilities					Pre-Challenger Operations With Incremental Development			Post-Challenger Revalidation Return-To-Flight			GPC Memory/Speed Upgrade CMM Level 5 Optimized Process Skill, Stable Workforce					Workforce Instability OI-25 PTI DR Escapes Process Change GPS Upgrade					Restore Workforce Stability Influx Of New Personnel					Cockpit Avionics Upgrade Post-Columbia Return-To-Flight			Shuttle Ending OI-32, OI-33, OI-34			Shuttle Ending Skill Maintenance Reductions-In-Workforce		
1978	1979	1980	1981	1982	1983	1984	1985	1986	1987	1988	1989	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011



Number Of Flights To FSW Severity 1 DR In-Flight

1978	1979	1980	1981	1982	1983	1984	1985	1986	1987	1988	1989	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011
Initial System Development Supports Incrementally STS-1, STS-2, and STS-5 With Major Capabilities					Pre-Challenger Operations With Incremental Development			Post-Challenger Revalidation Return-To-Flight			GPC Memory/Speed Upgrade CMM Level 5 Optimized Process Skill, Stable Workforce					Workforce Instability OI-25 PTI DR Escapes Process Change GPS Upgrade					Restore Workforce Stability Influx Of New Personnel					Cockpit Avionics Upgrade Post-Columbia Return-To-Flight			Shuttle Ending OI-32, OI-33, OI-34			Shuttle Ending Skill Maintenance Reductions-In-Workforce		
1978	1979	1980	1981	1982	1983	1984	1985	1986	1987	1988	1989	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011



- **Risk Level of 1 in 1000 at January 2006 established during reliability research in the late 1980's as a Return-To-Flight action. Variation over time based on prior chart, MTBF as calendar days between all DR's including DR's found during ground verification of future releases.**
  - **Computed Value For STS-1, 327 flights; For STS-134, 5260 flights.**

Summary Of Product DR By Period

Years	New Product DRs Introduced In Period	Latent, Unknown Product DRs At End of Period	Flight Days Over Period	DRs Occurring In Flight	Latent, Unknown Severity 1 DRs
1978-1982	523	424	29	3	4
1983-1985	109	322	147	8	6
1986-1988	16	240	None	No Flights	No Flights
1989-1993	22	140	291	1	0
1994-1997	12	100	365	4	0
1998-2002	8	39	675	2	0
2003-2005	0	20	None	No Flights	No Flights
2006-2008	1	2	162	1	0
2009-2011	0	N/A	114	0	0

- Supporting information available in more detail backup presentation.

Summary Of Quality Metrics By Period

Years	Product Error Rate DRs / KSLOC	Pre-Build Error Detection Effectiveness	Verification Effectiveness (Percent Found By SRR)	Notes
1978-1982	0.8 (STS-1) to 1.1	Information Not Available	77 % to 91 % (STS-1)	
1983-1985	2.8 (OI-1) to 1.1	40 % to 65 %	70 % to 80 %	Very Short Cycle - Release Every 4 Mo.
1986-1988	0.7 to 0.2 (OI-8C)	Near 80 %	60 % to 70 %	Return-to-flight Critical Changes
1989-1993	0.1 to 0.2	80 % to 90 %	80% to 90 %	
1994-1997	0.1 to 0.2 except 0.8 for OI-25	75 % to 85 %	85 % to 100 % except 60 % for OI-25	Isolated Process Escape on OI-25
1998-2002	0.1 to 0.2	85 % to 90 %	85 % to 95 %	
2003-2005	CAU Canceled	CAU Canceled	CAU Canceled	Work on CAU required changes, Later CAU Canceled
2006-2008	0.0 to 0.1	80 % to 100%	95 % to 100 %	
2009-2011	No OI Development	No OI Development	No Development	Reduced Flight System Changes Only, No OI Dev.

Summary Of Modeled Reliability By Period

Years	Calendar Days Between Any Product DR	Flight Days Between In-Flight DRs	Risk To Shuttle Due To Severity 1 FSW DR
1978-1982	6 (STS-1), 7 (STS-5)	7 (STS-1), 9 (STS-5)	1 in 327 (STS-1) to 1 in 409 (STS-5)
1983-1985	10 to 19	12 to 24	1 in 552 to 1 in 1072
1986-1988	29 at STS-26	90 at STS-26	1 in 1599 at STS-26
1989-1993	29 to 42	90 to 131	1 in 1599 to 1 in 2335
1994-1997	42 to 54	131 to 120	1 in 2335 to 1 in 3161
1998-2002	54 to 61	120 to 140	1 in 3161 to 1 in 3491
2003-2005	75 at STS-114	235 at STS-114	1 in 4212 at STS-114
2006-2008	75 to 88	235 to 276	1 in 4212 to 1 in 4930
2009-2011	88 to 94	276 to 294	1 in 4930 to 1 in 6260

- Risk level of approximately 1 in 1000 at January 2006 established during reliability research in the late 1980's as a Return-To-Flight action. Variation over time based on MTBF as calendar days between any Product DR's.

Historical PASS Quality Metrics

SYSTEM	KSLOCs	Major Errors	Early Detection (%)	Process		Product		Verification Detection (%)	Process Plus Product Error Rate DRs/KSLOC
				DRs	Error Rate (DRs/KSLOC)	DRs	Error Rate (DRs/KSLOC)		
R16 (STS-1)	350.0	N/A	N/A	2764	7.90	281	0.80	90.8	8.7
R-18 (STS-2)	78.0	N/A	N/A	617	7.91	91	1.17	87.1	9.1
R-19 (STS-5)	135.0	N/A	N/A	516	3.82	151	1.12	77.4	4.9
OI01	4.0	40	47.1	34	8.50	11	2.75	75.6	11.3
OI02	10.6	148	51.0	115	10.85	27	2.55	81.0	13.4
OI03	8.0	28	34.6	39	4.88	14	1.75	73.6	6.6
OI04	11.4	147	58.3	83	7.28	22	1.93	79.0	9.2
OI05	5.9	66	60.6	35	5.93	8	1.36	81.4	7.3
OI06	12.2	176	74.9	42	3.44	17	1.39	71.2	4.8
OI07	8.8	85	69.7	27	3.07	10	1.14	73.0	4.2
OI7C	6.6	40	63.5	10	N/A	13	N/A	N/A	3.5
OI8A	6.3	50	61.0	19	N/A	13	N/A	N/A	5.1
OI8B	3.1	25	83.3	3	0.97	2	0.65	60.0	1.6
OI8C	7.0	29	78.4	6	0.86	2	0.29	75.0	1.1
OI8D	12.1	32	71.1	11	0.91	2	0.17	84.6	1.1
OI8F	1.9	15	88.2	2	1.05	0	0.00	100.0	1.1
OI20	29.4	139	72.0	47	1.60	7	0.24	87.0	1.8
OI21	21.3	110	79.7	23	1.08	5	0.23	82.1	1.3
OI22	34.4	133	80.1	28	0.81	5	0.15	84.8	1.0
OI23	24.0	114	91.9	8	0.33	2	0.08	80.0	0.4
OI24	10.4	81	88.0	10	0.96	1	0.10	90.9	1.1
OI25	15.3	89	74.8	18	1.18	12	0.78	60.0	2.0
OI26	7.3	60	77.9	16	2.19	1	0.14	94.1	2.3
OI26B	11.0	67	85.9	10	0.91	1	0.09	90.9	1.0
OI27	12.1	61	87.1	9	0.74	0	0.00	100.0	0.7
OI28	6.7	46	86.8	6	0.90	1	0.15	85.7	1.1
OI29	26.8	507	88.2	62	2.31	6	0.22	91.2	2.5
OI30	14.6	105	84.7	18	1.23	1	0.07	94.7	1.3
OI32	7.0	54	91.5	5	0.72	0	0.00	100.0	0.7
OI33	8.0	61	80.3	14	1.74	1	0.12	93.3	1.9
OI34	1.2	6	100.0	0	0.00	0	0.00	N/A	0.0

Reliability Prediction Methods Used By PASS Software Process

Predict Software Reliability At Release (CI)

- In the late 1980's, the PASS FSW organization investigated reliability of the PASS FSW system using the "SMERFS" model.
- Two issues were identified in looking at predictions from "SMERFS' versus actual data:
  - The results that it produced seemed to skew the risk of a failure at the level of individual software release layers (individual OI's). Failures from oldest OI's were under predicted. Failures from recent OI's were over predicted. Totals were as expected.
  - "SMERFS" model required actual failure history to predict reliability. An alternate reliability model was developed to allow accurate predictions of reliability for a system prior to its release and hence prior to any actual failure history.
    - Model was developed in 1990
    - Model has been used on every PASS FSW release since then. Actuals versus predictions are presented to NASA customer semi-annually
- <u>Primary objective is monitor trend of changes to reliability, not predict absolute values</u>

OI-30 1st Flight to Last Flight Failure Estimates

- The data presents a prediction of software failures to be encountered from the 1st OI34 flight until the last OI34 flight by release increment where introduced.
- The prediction was made on 7/19/10 based on the updated manifest dates for STS-134 (launch 02/26/2011).
  - The expected number of failures was 6 (any Product DR found in execution), an average of one failure every 90 calendar days.
  - Of these failures, best estimate is that 4 will occur on pre-OI03 introduced changes.
  - 95 % Confidence Interval is the range from 42 days to 977 days between failures (Calendar Days between Any Product DR found as a failure)
- There have been no failures since the launch of the first flight off OI-34, a period of 325 days.

System Introduced Label	Expected Number of Failures	95% Probability Smallest Number of Failures	95% Probability Largest Number of Failures
STS-1	2.27	0.00	4.72
STS-2	0.52	0.00	1.07
STS-5	0.93	0.00	1.92
OI- 1	0.03	0.00	0.06
OI- 2	0.08	0.00	0.16
OI- 4	0.08	0.04	0.12
OI- 5	0.11	0.06	0.15
OI- 6	0.13	0.06	0.19
OI- 7	0.07	0.00	0.15
OI-8B	0.10	0.04	0.16
OI-8C	0.03	0.01	0.05
OI-8D	0.08	0.00	0.28
OI-20	0.11	0.00	0.40
OI-21	0.08	0.03	0.14
OI-22	0.11	0.08	0.14
OI-23	0.07	0.00	0.18
OI-24	0.03	0.01	0.06
OI-25	0.18	0.00	0.36
OI-26	0.04	0.01	0.07
OI-26B	0.05	0.01	0.08
OI-27	0.05	0.02	0.09
OI-28	0.07	0.02	0.12
OI-29	0.29	0.00	1.30
OI-30	0.12	0.04	0.21
OI-32	0.19	0.06	0.32
OI-33	0.20	0.06	0.34
OI-34	0.04	0.01	0.07
Total	6.06	0.56	12.91

Reliability Prediction Interpretation

- Reliability determined from the number of failures occurring during flight, KSC operations, SMS crew training, and OI development and verification testing (including SAIL)
- Failures should be a function of:
  - Total number of latent defects in the software
  - Relative magnitude of execution during a year (OI's in verification, special certification activities, number of crews in training, etc.)
- Improvement driven by reducing the number of latent defects in software while minimizing newly introduced defects