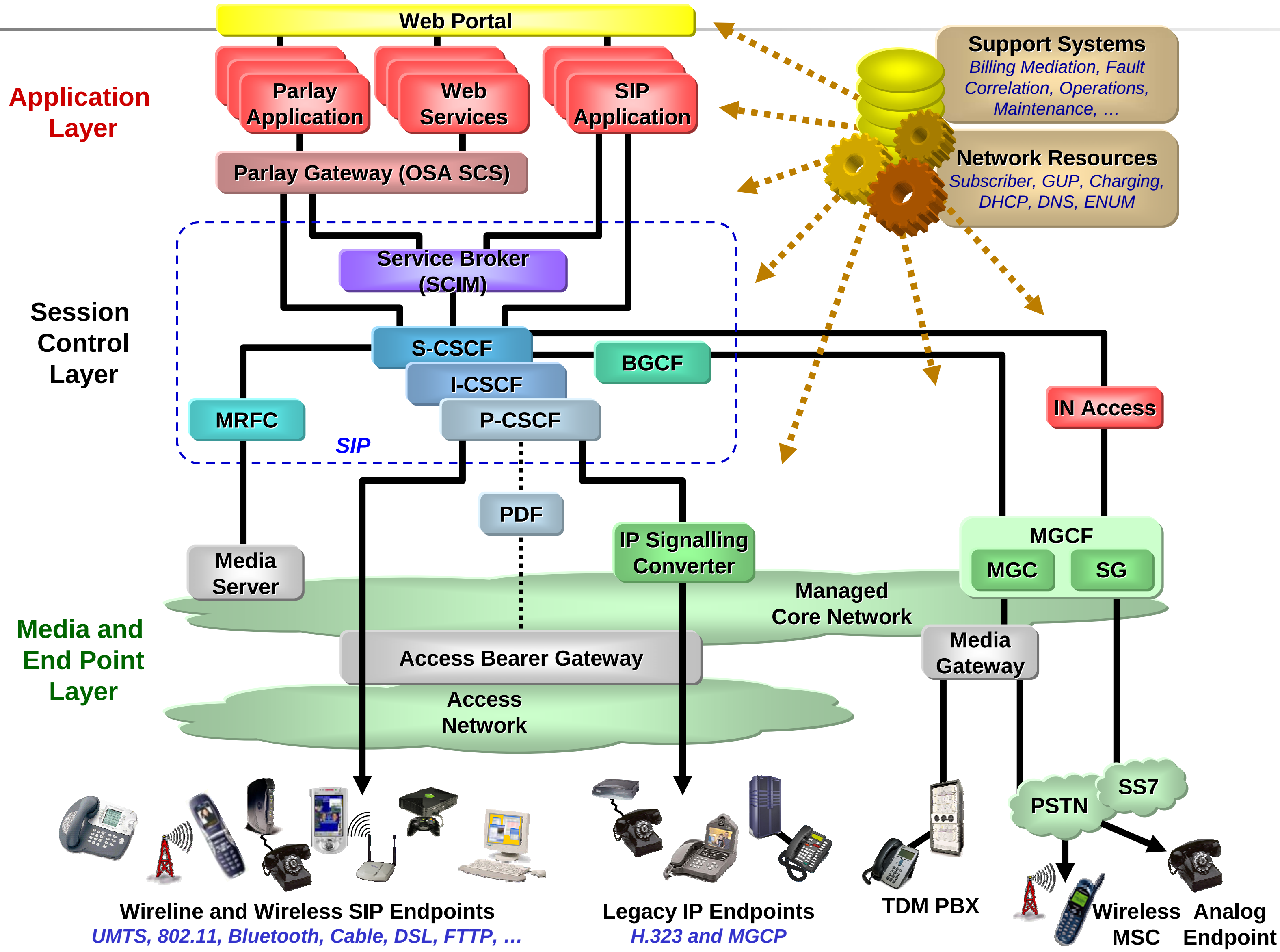
Architecting for Reliability – Detection Mechanisms

Robert S. Hanmer
Global Procurement
hanmer@alcatel-lucent.com

Veena B. Mendiratta
Chief Technology Office
veena@alcatel-lucent.com

Workshop on Architecting Dependable Systems **June 2008**

Today's Communication Network Using IMS Architecture



Alcatel·Lucent

Detection comes first

When errors occur they lie latent until detected.

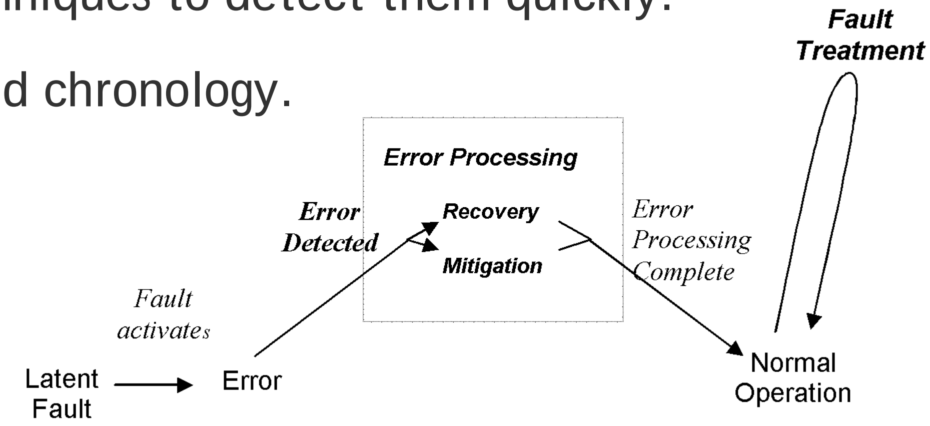
The speed of detection determines the speed of recovery and hence the availability.

Historical telecom systems were custom built and designed for high availability.

Modern networks utilize COTS components that might not be designed for high availability.

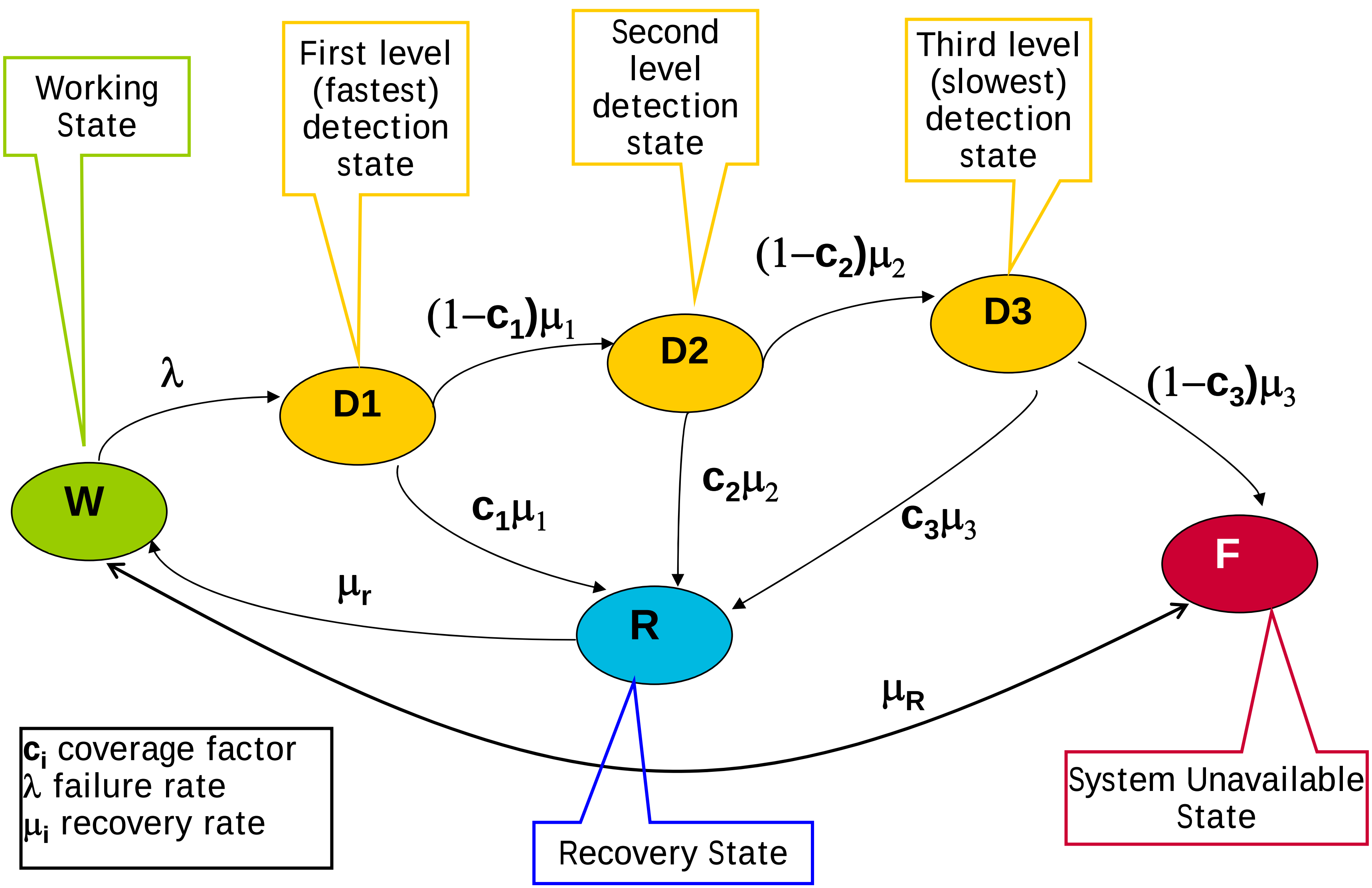
Different errors require different techniques to detect them quickly.

Techniques can be nested in scope and chronology.



Alcatel·Lucent

Reference Escalating Recovery Model



Alcatel·Lucent

Detection schemes ranked by steady-state probabilities

	Working (W)	Failed (F)	Detection+ Recovery (D+R)	F/(D+R)
Best	H H L	L H H	H H L	L H H
	H L H	H L H	H L L	H L H
↕	L H H	H H L	H L H	H H L
	H L L	H L L	L H L	L L H
	L H L	L H L	L H H	L H L
Worst	L L H	L L H	L L H	H L L

H indicates high coverage: modeled as 0.9
L indicates low coverage: modeled as 0.5

HHL indicates:
high coverage detection method, escalating to another high coverage detection method, that escalates to a low coverage detection method

Detection Techniques

Many different detection techniques are well known in the industry.

They have varying effectiveness, both in terms of completeness and speed.

Detection techniques by speed

Extremely fast	Medium fast	Long duration
Layer 1 protocol checkers	Watchdogs	Voting
Invalid arithmetic detection	Software-based protocol checkers	Routine correcting audits
Invalid address range detection	Complete parameter checking	Routine hardware exercises

Some example combinations:

- **HHH**: layer 1 protocol checker in hardware, then software protocol checker, then routine correcting audits. Highest availability but requires hardware support.
- **LHH**: Rudimentary COTS detection, then software protocol checking, then routine correcting audits. Typical of COTS, medium availability at best.

Conclusion and Next Steps

Escalating detection model allows analysis and consideration of design alternatives.

Availability is increased when high coverage extremely fast detection techniques are implemented. These techniques have highest cost and frequently require hardware assist, which is not possible in COTS hardware.

Compensating for fast low-coverage detection with slower higher-coverage techniques is not nearly as effective, but is sometimes necessary.

Next step

Extend the model to include other stages of recovery.

Thank you.

Steady state probabilities for model

	Detecting, D (D1+D2+D3)	Recovery (R)	(D+R)	Failed (F)	Working (W)	Not Up (1-W)	F/(D+R)
$c_1, c_2, c_3 = 0.5$	0.000980	0.000332	0.001312	0.001423	0.997265	0.002735	1.08
$c_1, c_2, c_3 = 0.6$	0.000665	0.000356	0.001021	0.000729	0.998250	0.001750	0.71
$c_1, c_2, c_3 = 0.7$	0.000412	0.000370	0.000782	0.000308	0.998910	0.001090	0.39
$c_1, c_2, c_3 = 0.8$	0.000222	0.000377	0.000599	0.000091	0.999310	0.000690	0.15
$c_1, c_2, c_3 = 0.9$	0.000095	0.000380	0.000475	0.000011	0.999514	0.000486	0.02
L: c_i = 0.5; H: c_i = 0.9							
H L L	0.000222	0.000371	0.000593	0.000285	0.999122	0.000878	0.48
H H L	0.000095	0.000378	0.000473	0.000057	0.999469	0.000531	0.12
L L H	0.000981	0.000370	0.001351	0.000285	0.998363	0.001637	0.21
L H H	0.000349	0.000378	0.000727	0.000057	0.999216	0.000784	0.08
H L H	0.000222	0.000378	0.000600	0.000057	0.999343	0.000657	0.10
L H L	0.000348	0.000371	0.000719	0.000285	0.998996	0.001004	0.40