Qualities

Reliability

Does your modelling ensure reliability ?

Niels Malotaux

N R Malotaux Consultancy

+31-655 753 604 niels@malotaux.nl www.malotaux.nl

Niels Malotaux

Project/team/organization Coach

Helping projects and organizations to quickly become

- More effective - doing the right things better
- More efficient - doing the right things better in less time
- Predictable - delivering as needed

Getting projects back on track

Helping with Architecture/Design/Review
of electronics/firmware/software

Project types
electronic products,
firmware, software,
space, railway, telecom,
industrial control,
parking system

Reliability

- The product simply works, and keeps working
- How do we know it will ?

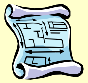
Predicting Reliability ?

- If you can predict reliability,
  you know what will fail, so you *can prevent it*
- If you don't know what will fail, you *cannot predict reliability*
- Testing does not ensure reliability – it must be there *by design*

- To record our design thinking and decisions, we keep a DesignLog
- We ask others to review, because we know we're not perfect
- Are our designs reviewable ?

DesignLog

- In computer, not loose notes, not in e-mails, not handwritten
  - Text
  - Drawings!
  - On subject order
  - Initially free-format
  - For all to see
- All concepts contemplated
  - Requirement
  - Assumptions
  - Questions
  - Available techniques
  - Calculations
  - Choices + reasoning:
    - If rejected: why?
    - If chosen: why?
- Rejected choices
- Final (current) choices
- Implementation

<u>Chapter</u>
Requirement → What to achieve
.
Assumptions
Questions + Answers
.
.

.
.
Design options
Decision criteria
Decision → implementation spec

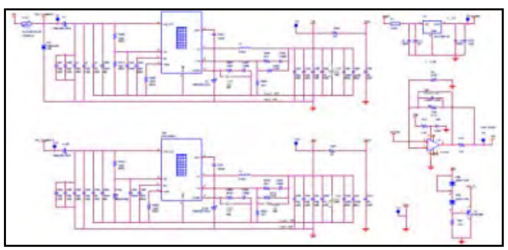
New date: change of idea:
Design options
Decision criteria
Decision → <u>implementation spec</u>

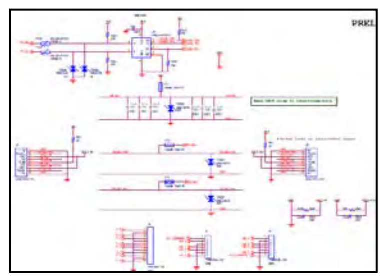
Art

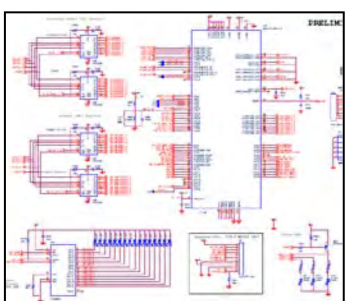
Sorry, picture removed for confidentiality

Hardware design

DesignLog: Resistance measurement

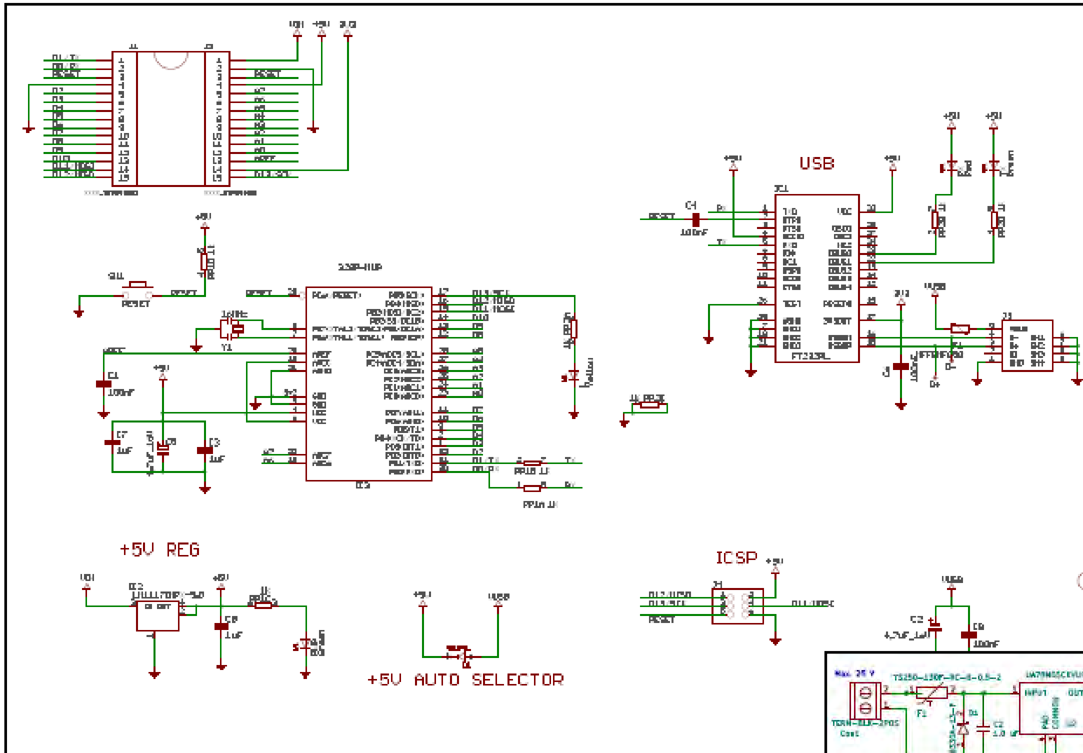


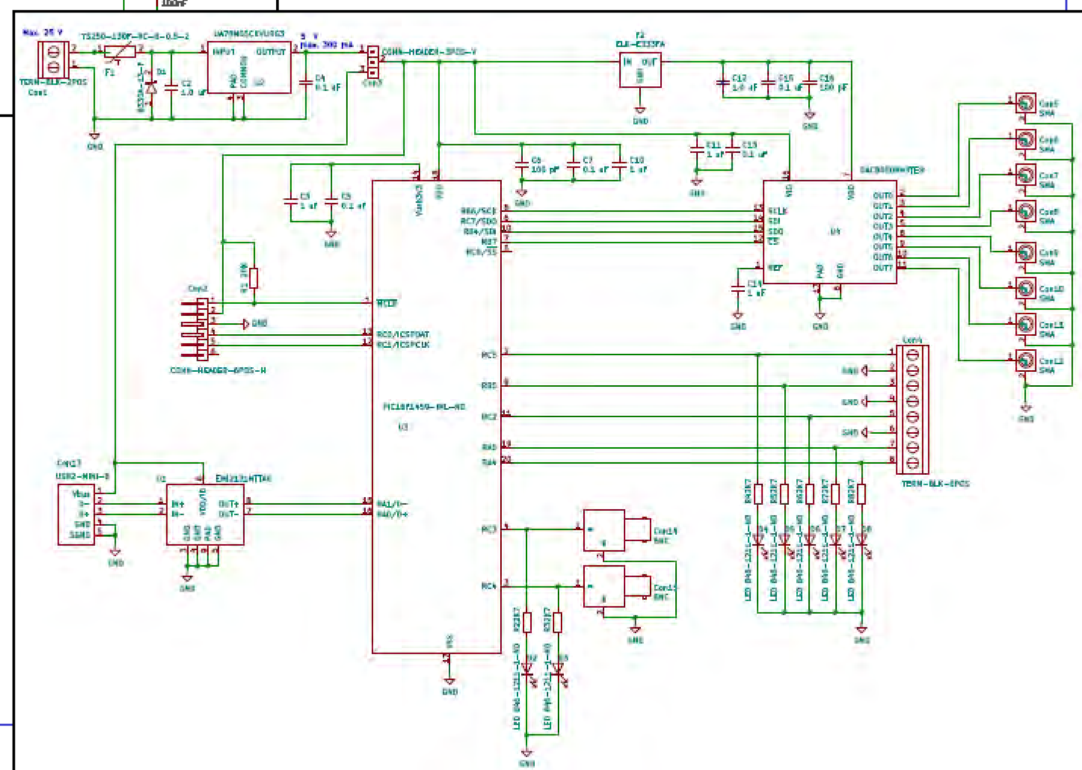




Sorry, some pictures removed for confidentiality

Schematic diagrams

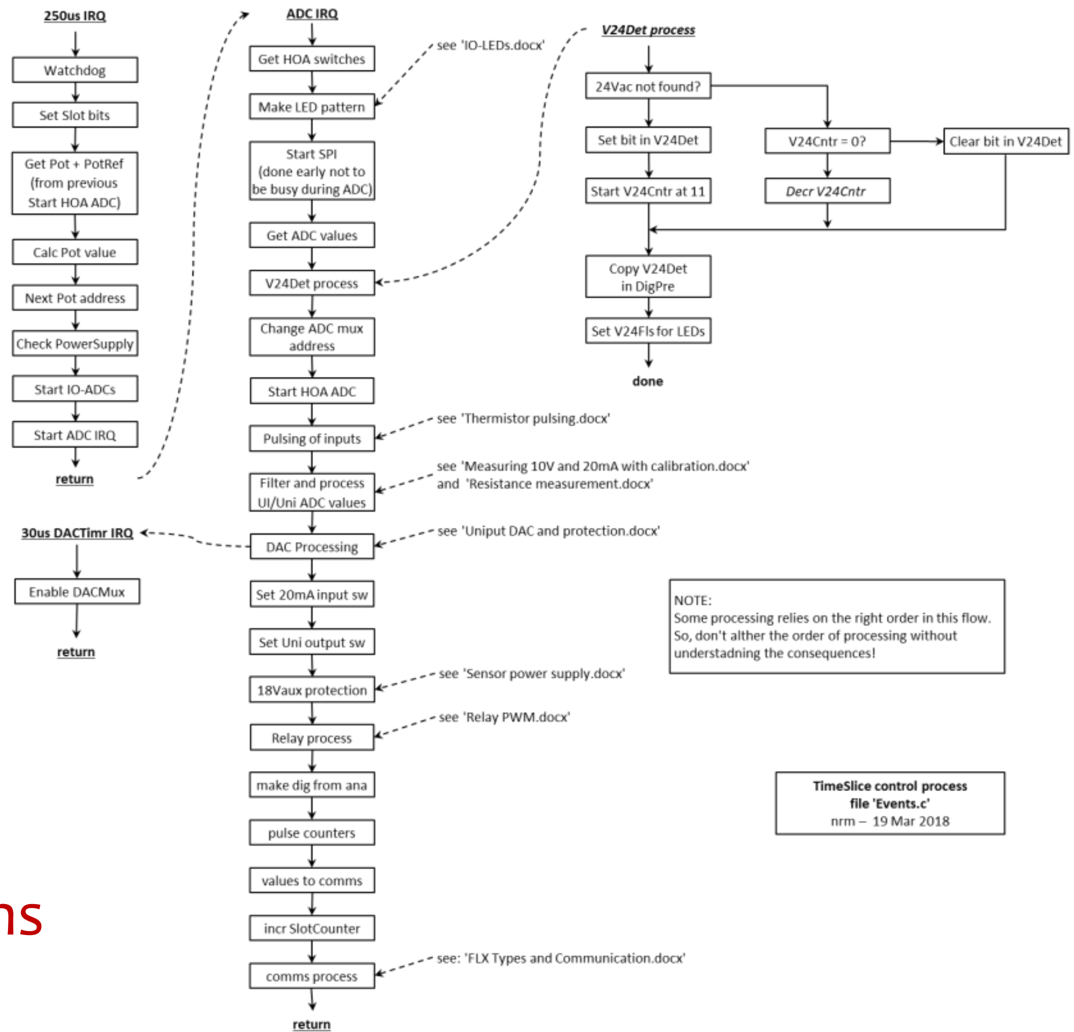




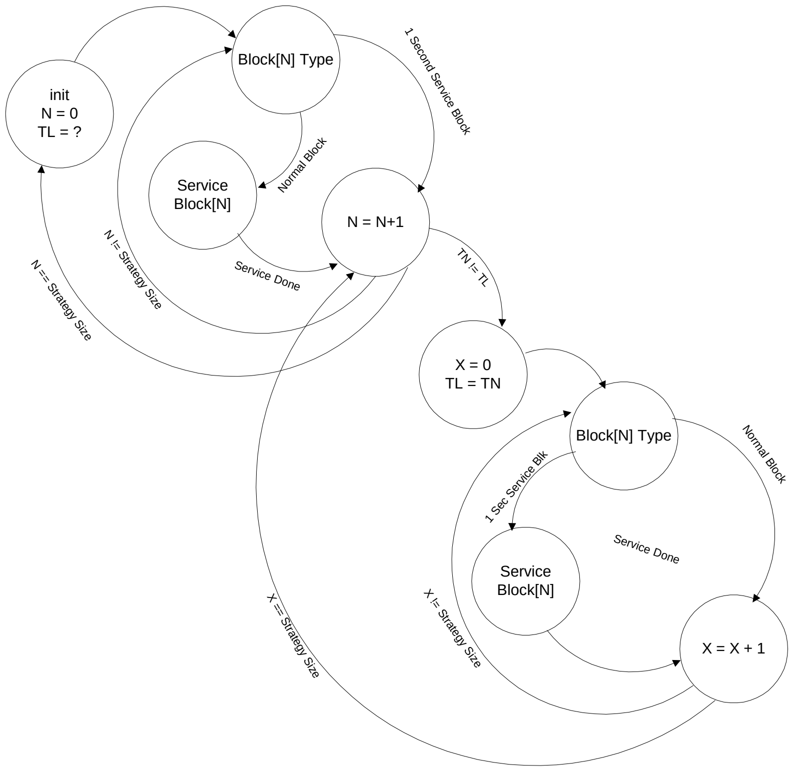
- Which one
  is easier to read ?

Firmware design

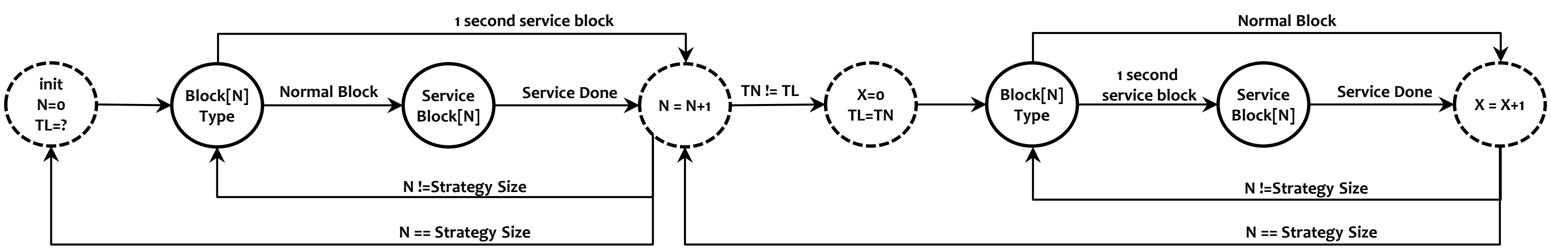
- Same every 250µs
- 8 x 250µs = cycles of 2ms



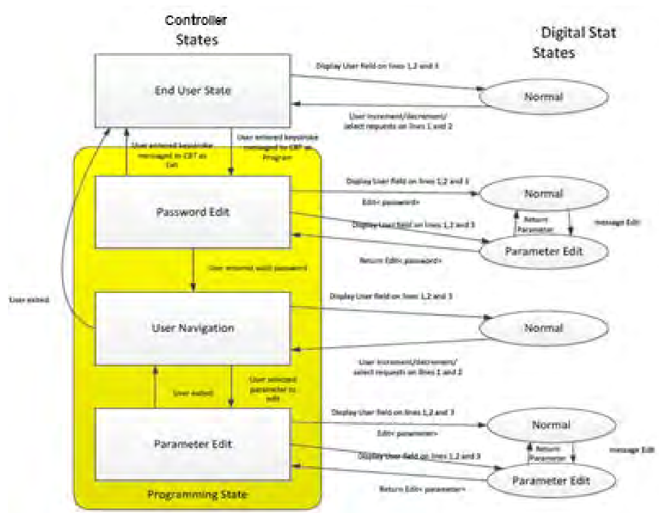
There are many ways to represent a design

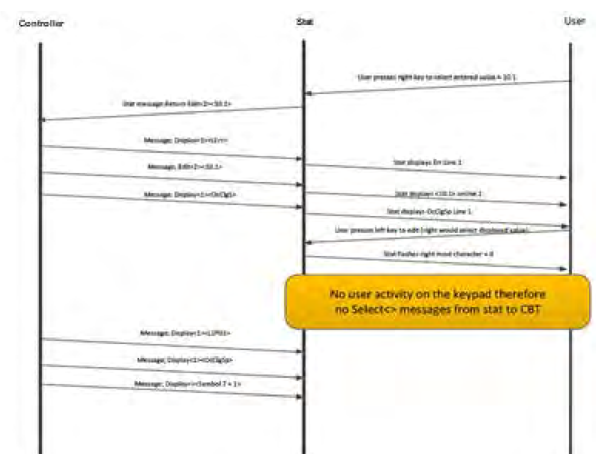


- Only few are useful
- Which one is easiest to follow ?
- Don't waste reviewer's time



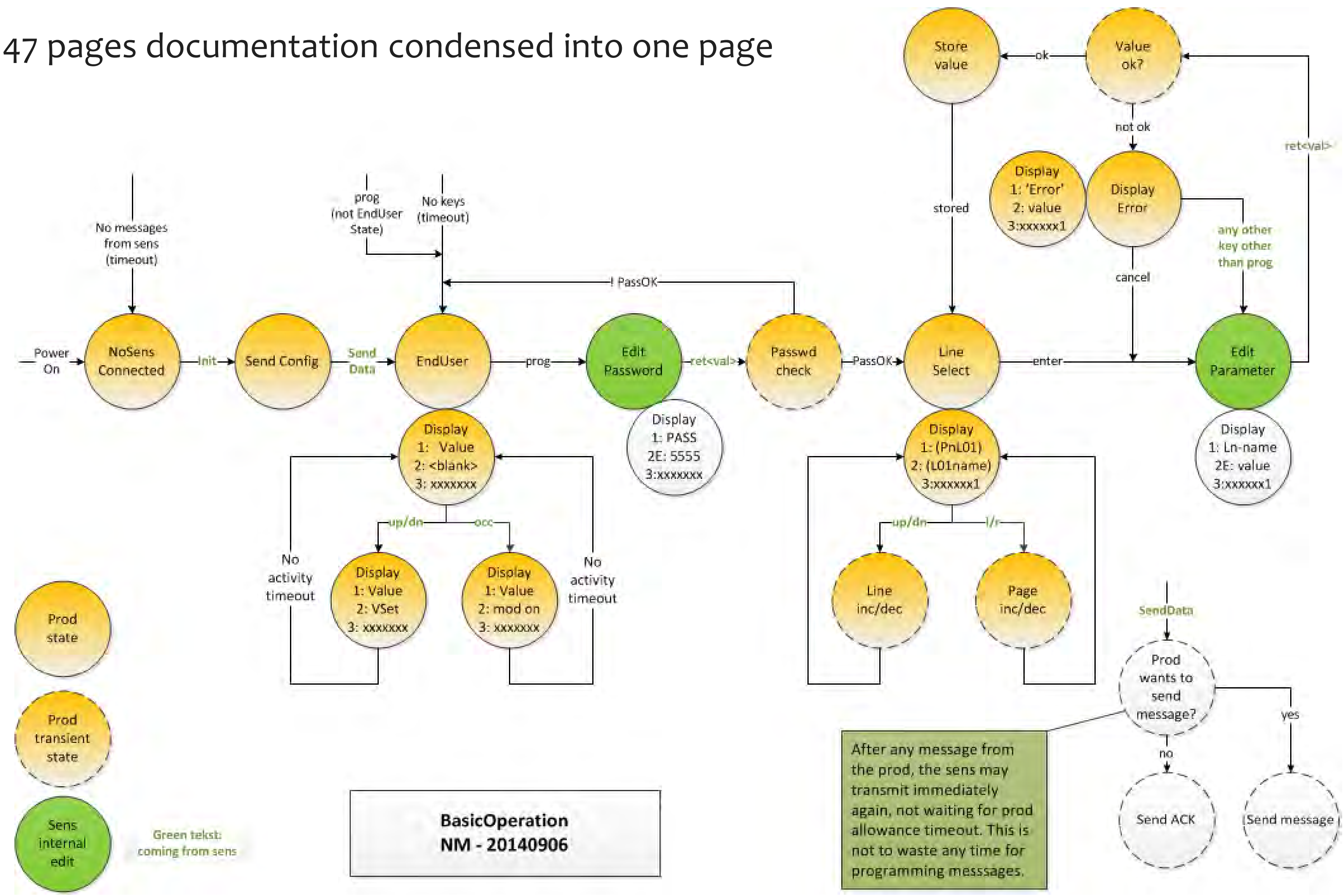
Useful design ?



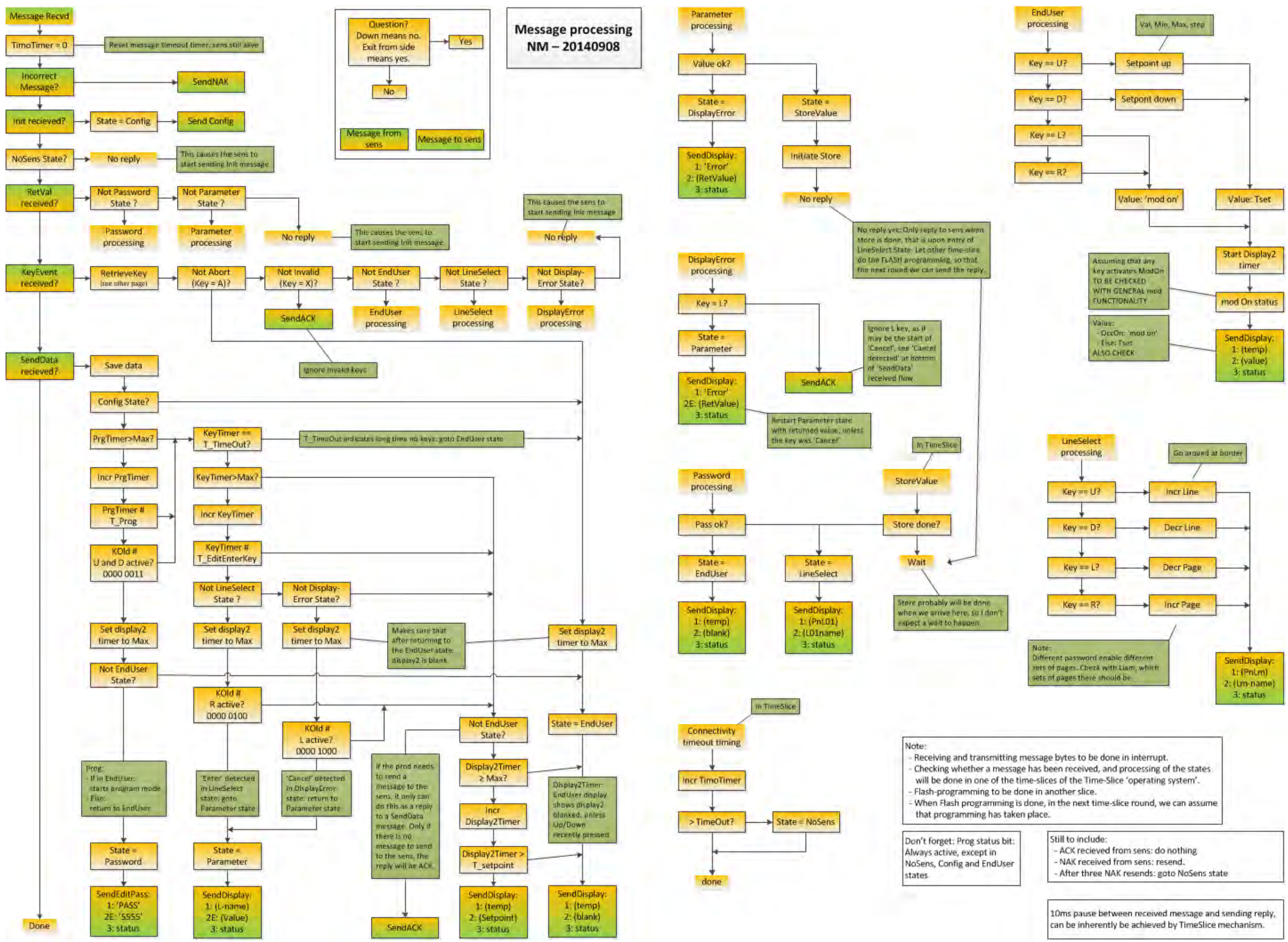


Choose the appropriate design

47 pages documentation condensed into one page



Design example



How about your models ?

- Reviewable at one glance ?
- Not a puzzle ?
- What do they look like ?
- Will they ensure reliability ?

Qualities

Reliability

Does your modelling ensure reliability ?

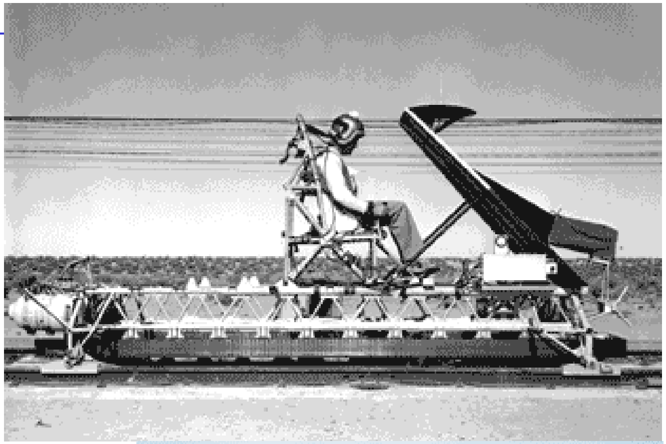
Niels Malotaux

N R Malotaux
Consultancy

+31-655 753 604 niels@malotaux.nl www.malotaux.nl

MTBF

Predicting reliability ?

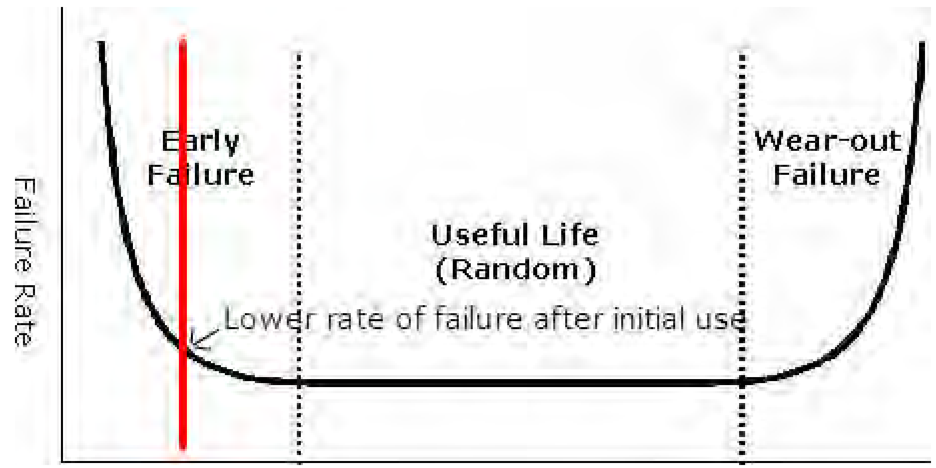


- If we can predict (un)reliability, we can do something about it
- Murphy's Law:
  - Whatever can go wrong, will go wrong
- Should we accept fate ??

- Murphy's Law for Professionals:
  - Whatever can go wrong, will go wrong …

  Therefore
  - We should actively check all possibilities that can go wrong and make sure that they cannot happen

Reliability - Calculating MTBF ?



- Assume MTBF 10 year
  - How many of the systems produced still work properly after 10 year ?
  - $p(t) = e^{-t/MTBF}$
  - If t = MTBF, then $e^{-1} = 36.8\%$
- Meaningless exercise,
  producing impressive tables full of numbers
- Product should simply still be working

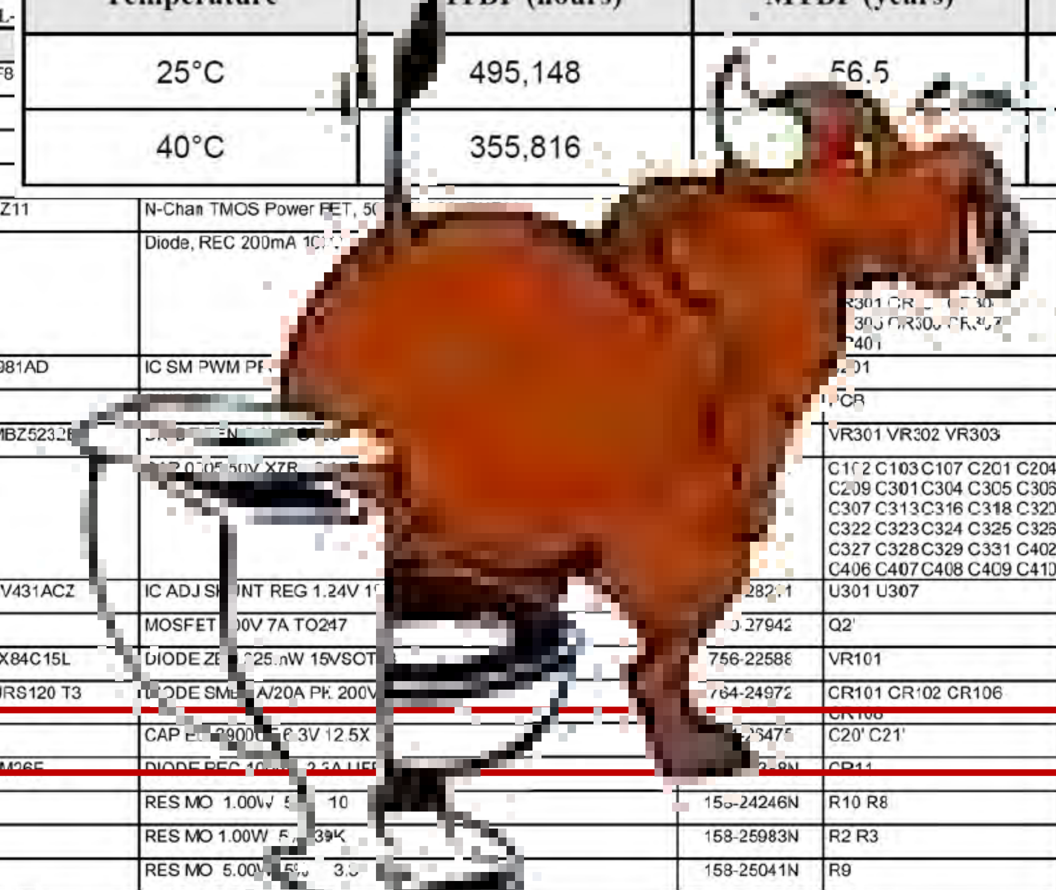
Impressive numbers

MTBF Prediction Report

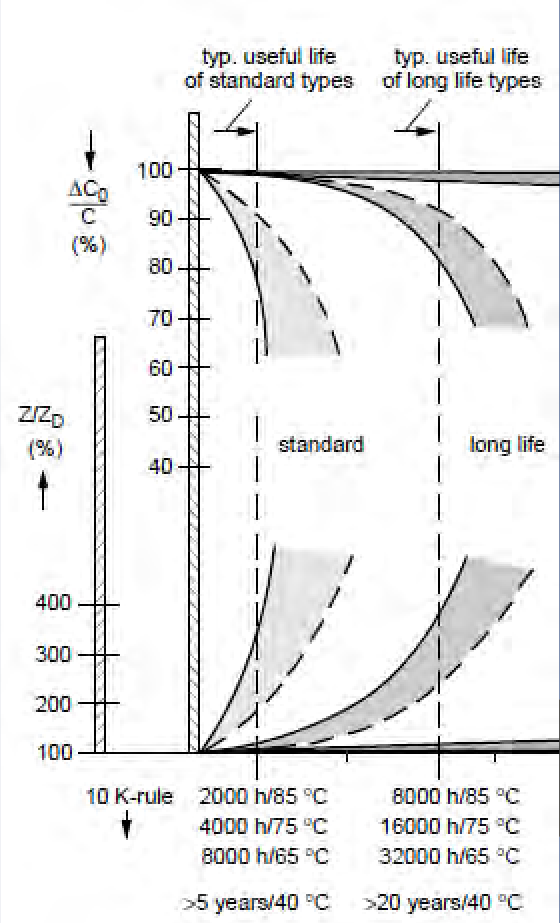
P/N Detail, Sorted by TFR

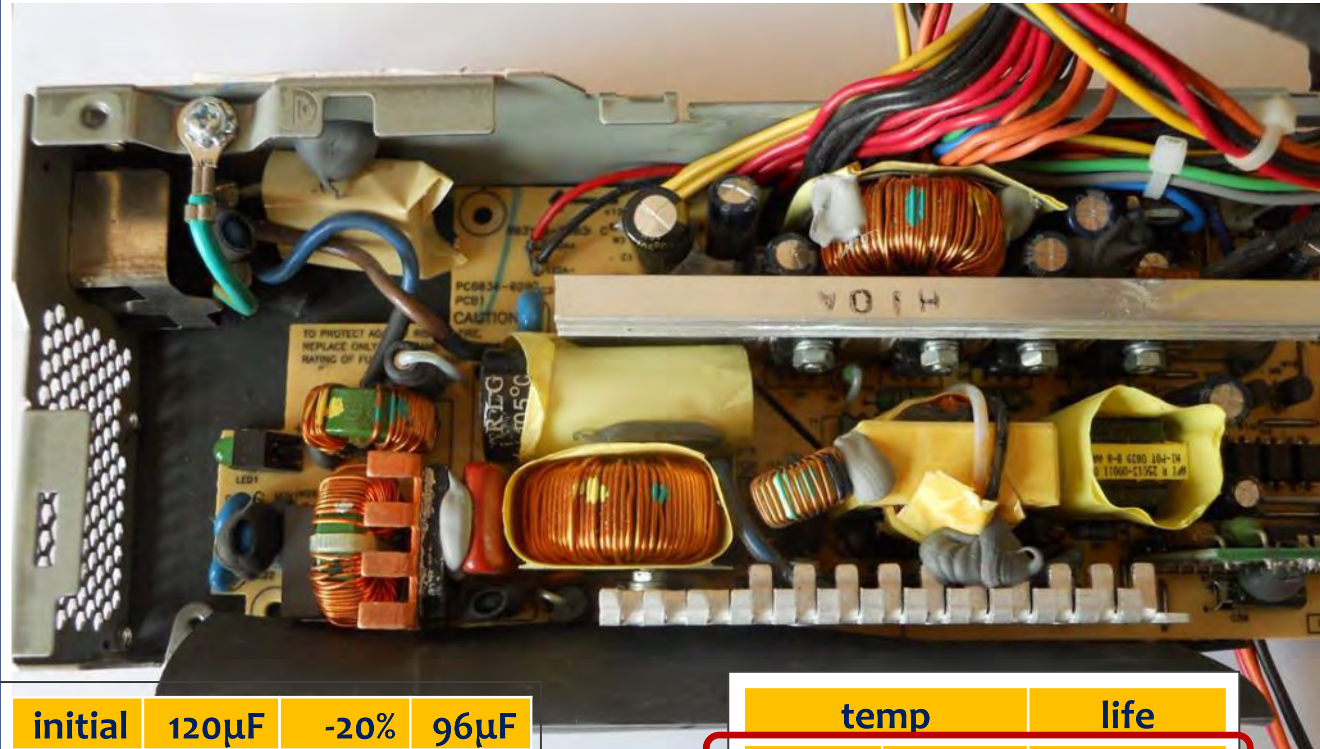
Temperature	MTBF (hours)	MTBF (years)	Failure Rate (FIT)
25°C	495,148	56.5	2020
40°C	355,816	[illegible]	2810

P/N:
Environment: MIL-



Category								Rise (C)	Stress (%)
	IRF8	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	18	23
		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	56	na
		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	15	na
		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	0	5
	BUZ11	N-Chan TMOS Power FET, 50	[illegible]	[illegible]	1	85.36857	85.36857	31.3	na
		Diode, REC 200mA 10	[illegible]	R301 CR… 303 CR30… CR307 …401	16	3.91002	62.56032	5.5	50
	L4981AD	IC SM PWM PF	[illegible]	…201	1	[illegible]	[illegible]	[illegible]	na
		[illegible]	[illegible]	PCB	1	[illegible]	[illegible]	[illegible]	na
	MMBZ5232B	[illegible]	[illegible]	VR301 VR302 VR303	3	[illegible]	[illegible]	[illegible]	50
		CAP 0805 50V X7R	[illegible]	C102 C103 C107 C201 C204 C209 C301 C304 C305 C306 C307 C313 C316 C318 C320 C322 C323 C324 C325 C326 C327 C328 C329 C331 C402 C406 C407 C408 C409 C410	30	[illegible]	[illegible]	[illegible]	0
	LMV431ACZ	IC ADJ SHUNT REG 1.24V 1	…282…1	U301 U307	2	[illegible]	[illegible]	[illegible]	na
		MOSFET …00V 7A TO247	…27942	Q2'	1	[illegible]	[illegible]	[illegible]	50
	BZX84C15L	DIODE ZE… 225mW 15VSOT	756-22588	VR101	1	33.61112	33.61112	62.3	49.8
	MURS120 T3	DIODE SM… A/20A PK 200V	764-24972	CR101 CR102 CR106 CR108	4	8.318298	33.27319	3.3	50
		CAP EL 3900… 6.3V 12.5X	…23475	C20' C21'	2	12.64947	25.29895	30	52.4
	BYM26E	DIODE REC 10… 2.3A UF	…8N	CR11	1	23.6703	23.6703	27.5	2.4
		RES MO 1.00W 5… 10	158-24246N	R10 R8	2	10.42417	20.84835	5	50
		RES MO 1.00W 5… 39K	158-25983N	R2 R3	2	10.42417	20.84835	5	50
		RES MO 5.00W 5… 3.3	158-25041N	R9	1	19.5272	19.5272	10	50
	BYV26C	DIODE PW 600V 1.0A …PER	111-22734N	CR2	1	19.174	19.174	30	50
	MURH860CT	DIODE CT CC 600V 8A UFR TO220	140-27048	CR3'	1	18.0969	18.0969	28	4
	MMBZ5248BL	Diode, ZNR 18V SM SOT-23	756-27418	CR114 VR102	2	8.960463	17.92093	5.5	50
		CAP EL 150uF 400V 25X30	101-28694	C12'	1	2.909139	2.909139	22	3
	[illegible]	[illegible]	[illegible]	CR3'	1	[illegible]	[illegible]	[illegible]	[illegible]





initial	120µF	-20%	96µF
life	96µF	-20%	77µF

		Radial	4~50	0.1~330	-40 ~ +85
		Radial	6.3~50	0.1~330	-40 ~ +105
		Radial	4~50	0.1~330	-40 ~ +85
RSM	105°C,5mm L Height, Super Miniature, 1000hrs	Radial	6.3~50	0.1~220	-40 ~ +105
General					
ADF	55°C, For Photo Flash	Radial	330	80~300	-20 ~ +55
REB	105°C,Suited for ballast applications	Radial	160~450	10~330	-25 ~ +105
RGP	105°C, General ,1000hrs	Radial	6.3~450	0.1~22000	-40 ~ +105
RGU	85°C,General, Miniaturized,2000hrs	Radial	6.3~450	0.1~22000	-40 ~ +85
RLG	105°C,General , For Switching Power Supply,2000hrs	Radial	6.3~100	0.1~15000	-55 ~ +105
RLG	105°C,General, For Switching Power Supply, 2000hrs	Radial	160~250	0.47~470	-40 ~ +105
RLG	105°C,General , For Switching Power Supply,2000hrs	Radial	350~450	0.47~180	-25 ~ +105
RLH	105°C,General , For Switching Power Supply,3000hrs	Radial	160~450	3.3~220	-25 ~ +105
RLL	105°C,Low Leakage Current	Radial	6.3~100	0.47~3300	-40 ~ +105
Low ESR					

temp		life
105°C	85°C	2000 hr
95°C	75°C	4000 hr
85°C	65°C	1 yr
75°C	55°C	2 yr
65°C	45°C	4 yr
55°C		8 yr
45°C		16 yr

Unreliability by design

How leaders in the electronics industry handle MTBF

- Find a low-grade engineer
  (rationale: so critical resources are not used in this process)
- Ask the customer what MTBF would they like?
  10 years? 50,000 hours?
- Various adjustments are made in the MTBF calculations to provide the customer with the exact MTBF they require, plus a few additional thousand hours for a nice margin
- Move on with best practices in design reviews and verification, supplier assurance, process control, reliability prediction, and life testing to ensure optimum reliability of the product

Failures: Un-reliability

ref Albertyn Barnard

- All non-conformances are caused
  Anything that is caused can be prevented Crosby 1995
- Failures in electronic equipment have a traceable and preventable cause and may not be satisfactorily explained as some statistical inevitability Pascoe 2011
- Failures are primarily caused by
  errors made by design and production personnel
- Failures due to human nature and complexity of engineering and perhaps ignorance

Reliability

ref Albertyn Barnard

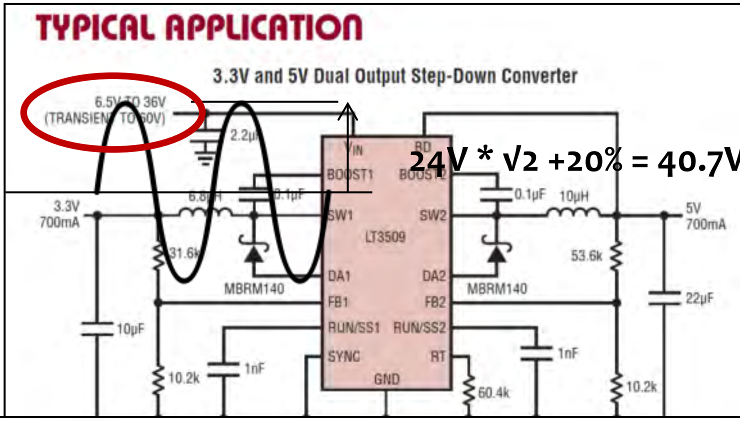
- Reliability is the absence of failures in products
  within its expected life under the full range of conditions experienced
- Reliability engineering is the function that
  prevents the creation of failures in products
  failure-free state can only be achieved if failure is prevented from occurring

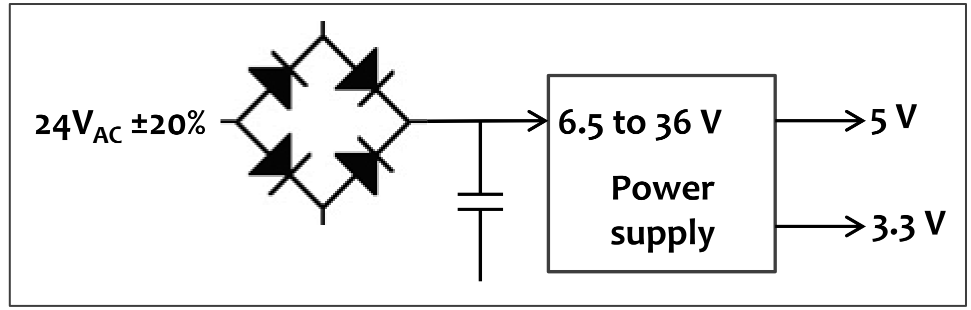
- If you can predict reliability,
  you know what will fail, so you *can prevent it*
- If you don't know what will fail, you *cannot predict reliability*
- Testing does not ensure reliability – it must be there *by design*

Dilution of Reliability ?

If the spec doesn't cover what the product is for,
don't simply implement the spec

Supply Requirements	24 V AC ±20% 50/60 Hz
Transformer Rating	up to 55 VA (up to 12 VA internal power plus up to 43 VA supplied to Triac loads)





LT3509

ELECTRICAL CHARACTERISTICS The ● denotes the specifications which apply over the full operating temperature range, otherwise specifications are at $T_A = 25°C$, $V_{IN} = 12V$. (Note 3)

PARAMETER	CONDITIONS		MIN	TYP	MAX	UNITS
V_{IN} Undervoltage Lockout				3.3	3.6	V
V_{IN} Overvoltage Lockout			37	38.5	40	V
Input Quiescent Current	Not Switching $V_{FB} > 0.8V$					mA
Input Shutdown Current	V(RUN/SS[1,2]) < 0.3V					µA
Feedback Pin Voltage		●	0.784	0.8	0.816	V
Reference Voltage Line Regulation	$3.6V < V_{IN} < 36V$			0.01		%/V

Datasheets are a contract !

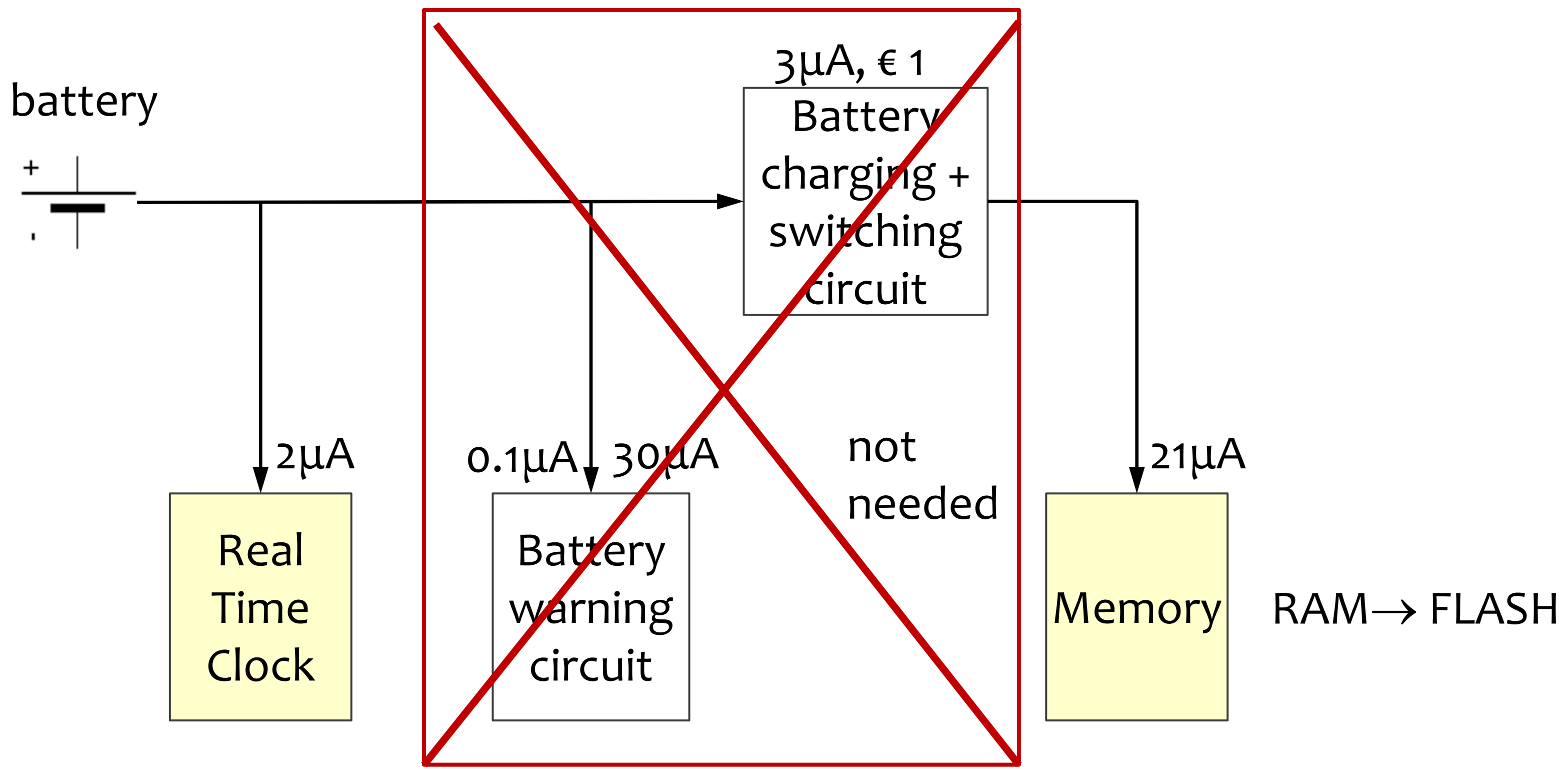
Supply Requirements	24 V AC +10% / -20% 50/60 Hz
Transformer Rating	up to 55 VA (up to 10 VA internal power plus up to 45 VA supplied to Triac loads)

No battery

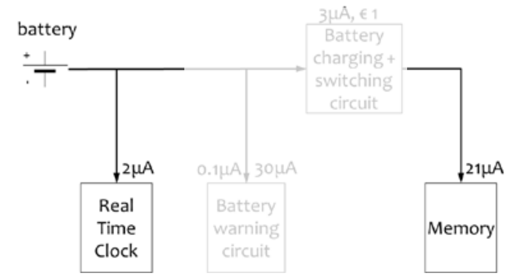
Should we always do
what the customer says ?

No battery ?

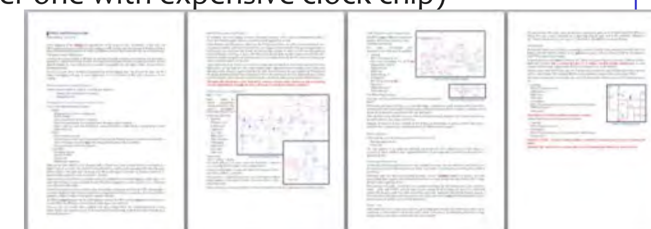
CR2032 battery	10yr >90% left	225mAh	
Total with memory	Old system	26μA	1 yr
Total with memory	Newer systems	56μA	5 mo
Clock in μC		2μA	12 yr
Separate clock chip (€0.5)		0.5μA	>12yr



No battery ?



- Using a few times "Why ?"
  - Boss: Because the competition boasts 'no battery'
  - Field sales people: We have to replace the battery every two year
  - Actual requirement: No need to replace the battery
- Boss said: SuperCapacitor
  - Endurance : +85°C 6000 h (more than 10 years at 40°C, we need 12 yr, 70°C)
  - Can keep clock running for almost 4 days (requirement >72 hr) → ok
  - Cost: $10 (40% of our total component budget*!* Competition uses cheaper one with expensive clock chip)
- NiCad rechargeable battery
  - Usable temp < 40°C ; not allowed anymore anyway
- Sony rechargeable Li battery
  - -40°C … 85°C, perhaps good enough, even for 4 days memory retention
  - Sony couldn't guarantee lifetime more than 4 yr (competition uses even less life type)
  - Cost: $1.50
- CR2032 coin cell
  - Endurance: 12 yr ok, if < 2µA; if limit to 2µA max, no need to replace battery
  - Cost: $0.23
- Do customers care about components used ? (Don't give me your solution. Give me your requirement)
  - Design log of 4 pages shows the design reasoning and decision



DesignLog

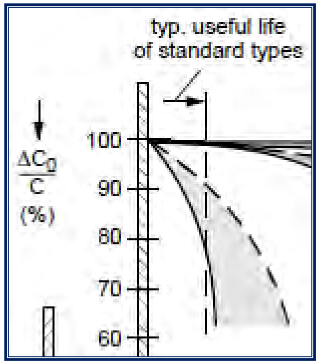
Decision Support

Should we do more tests ?

Don’t waste time if it won’t change the decision

Case: Thousands of products in the field

- Failures started coming in after some 5 year
- Electrolytic capacitors lost capacitance almost completely
- External lab: X-rayed, opened, expensive report compiled
- What was the specified life time ?
  - 8 or 10 yr ? I don't know what the boss wants
  - Boss: 12 year
- At which temperature ?
  - Specified: 50°C ambient
  - What does this mean for the component temperature ?
- 5 yr ≈ 44000 hr
  - 85°C, 2000hr capacitor used at 45°C is at -20% after some 4 yr



Temp		life
105°C	85°C	2000 hr
95°C	75°C	4000 hr
85°C	65°C	1 yr
75°C	55°C	2 yr
65°C	45°C	4 yr
55°C		8 yr
45°C		16 yr

Which decision do we have to make ?

- Let's do some more temperature tests !
  - What is the decision to make based on this ?
  - Would that decision change if we do more analysis ?
  - "I don't know. I don't know what the boss wants !"
  - Did you ask ?
  - How many products in your tests did show the problem ? Some 30%
  - If you do more tests, will that become less or more ? More like 50%, I think
- Decision choice
  - Tell all users: preemptive repair
    - "There is a small chance that these products may exhibit some problems in the future"
  - Repairing when a customer complains
- Boss' decision criterion ?
  - << 1% will return: repair on complaint
  - Otherwise: preemptive repair
- Hence: no point in spending time on more analysis
- Cheap parts can be very expensive – Quality costs less

Predictability feeds reliability

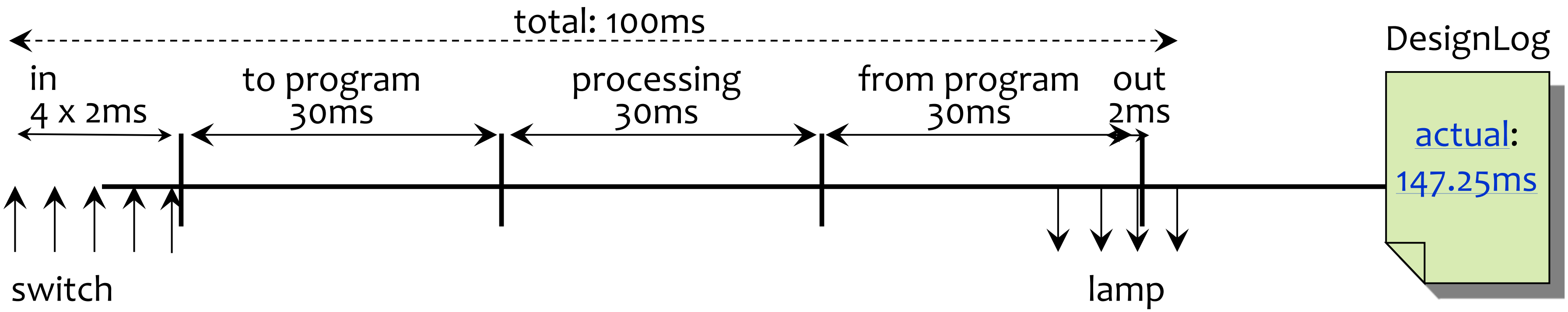
Conflicting system qualities ?

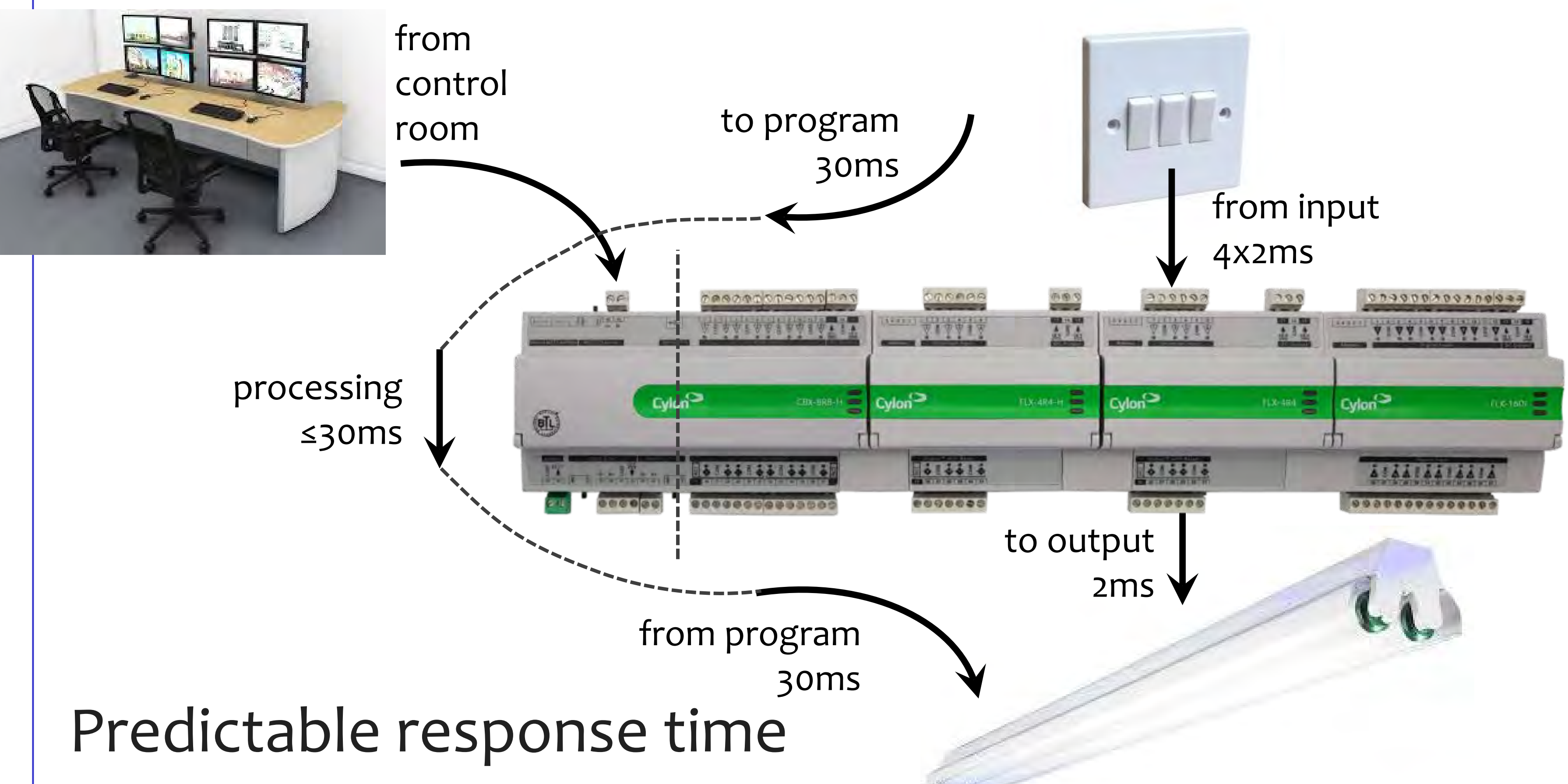
Architecture and design is finding an optimum compromise
between conflicting requirements

50°C, means 70°C in box

- Qualities:
  - Useful life — 12 yr
  - Ambient temperature — -25 °C … 50°C
  - Power supply — 24V ±20%
  - Response performance — goal < 100ms, tolerable < 150ms (250ms ??)
  - Precision — ±0.5% , temperature ±0.3°C
    (not clearly specified, but implied)
  - No battery (clock, memory) — use 'super cap'
- Within limited budgets
  - Component cost — ≤ $25
- And timescales
  - Production — asap, ≤ one year

    Delivery time more important than development cost
    Credibility of the company was on the line





Predictable response time