Xen and the Art of Certification

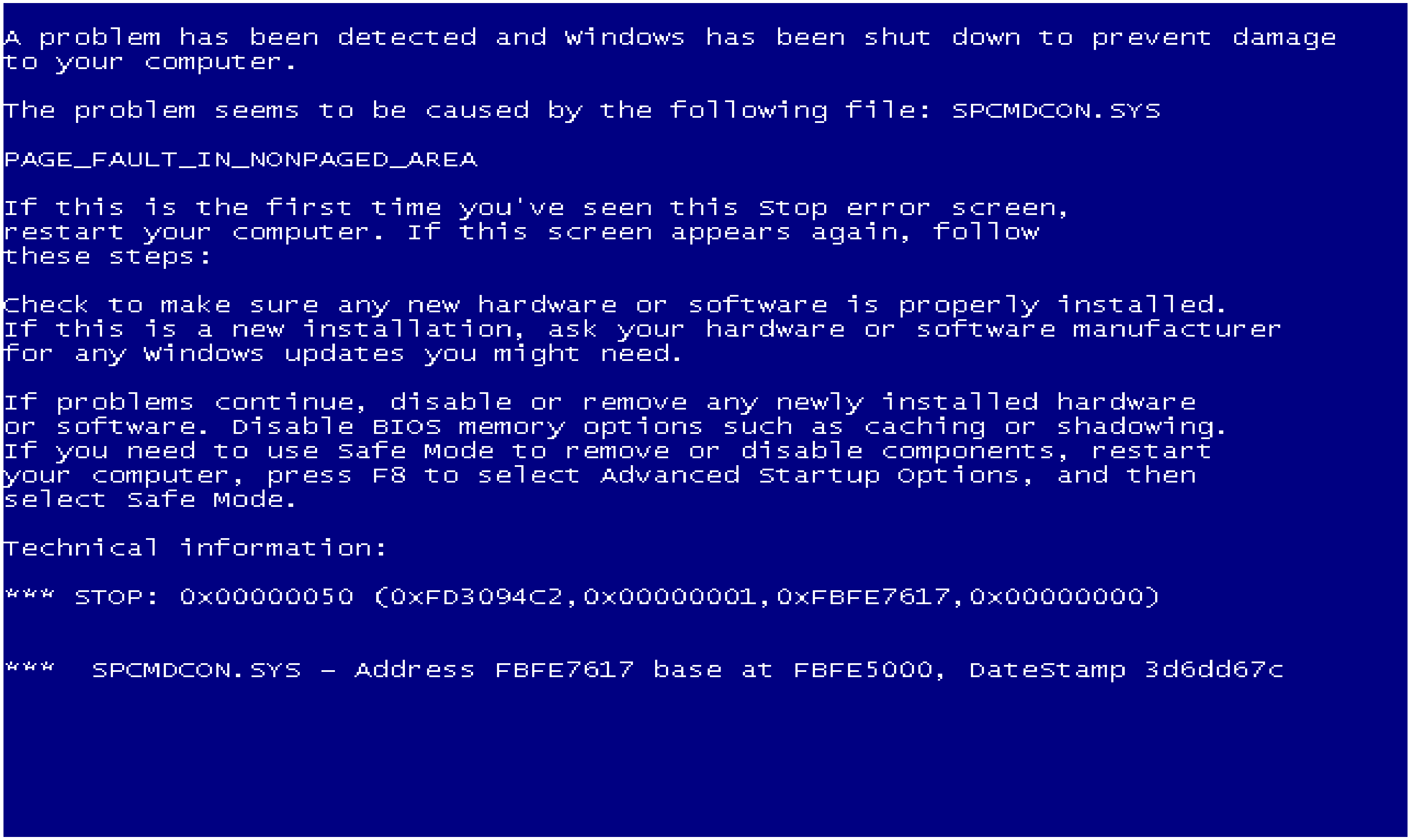
Nathan Studer and Robert VanVossen

Xen Developer Summit 2014

Certification – Why?

B787-2139 by MilborneOne is licensed under http://creativecommons.org/licenses/by-sa/3.0/deed.en

Certification – Why?



```
A problem has been detected and windows has been shut down to prevent damage
to your computer.

The problem seems to be caused by the following file: SPCMDCON.SYS

PAGE_FAULT_IN_NONPAGED_AREA

If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Technical information:

*** STOP: 0x00000050 (0xFD3094C2,0x00000001,0xFBFE7617,0x00000000)


***  SPCMDCON.SYS - Address FBFE7617 base at FBFE5000, DateStamp 3d6dd67c
```

Earning Trust

- Assurance standards /= “No Bugs” standards
- Demonstrate that your software can be trusted
- This trust is required for Medical, Automotive, and Aviation applications

Importance

- Server flaws do not usually cause direct personal harm.
- Flaws in safety-critical systems can kill
  - Car: Controlled Fireball
  - Plane: Passenger Carrying Missile
  - Robotic Surgery: Tamed Terminator

Overview

- **DornerWorks Work**
- Certification
- Certifying Core Xen
- Patch Examples
- Beyond Core Xen
- Cost
- Conclusion
- Questions

DornerWorks Work

- Started with the ARINC653 scheduler
- Continued with support by Navy Small Business Innovative Research (SBIR) topics
  - Rockwell Collins
  - Leanna Rierson – Designated Engineering Representative (DER)
  - Accuvant

DornerWorks Work

- Main Goals
  - Demonstrate Xen on Embedded Platforms
  - Understand what certifying Xen to DO-178 Design Assurance Level (DAL)-A and Common Criteria (CC) Evaluation Assurance Level (EAL) 6+ would take
  - Begin the certification process
  - Do some Formal Methods Analysis on Xen

Overview

- DornerWorks Work
- **Certification**
- Certifying Core Xen
- Patch Example
- Beyond Core Xen
- Cost
- Conclusion
- Questions

What is certification

- Requires things that everyone knows should be done, but tend to skip. (e.g. Documentation)
- Enforces good practices. (e.g. design and test independence)
- Interesting Verification Activities
- Prevent certification loopholes. (e.g. tool qualification)

Tool Qualification

- Normal Software Engineering Reflex: Automation.
- What if the automated tool introduces an error?

What is Required?

- What does each level require
  - DAL-E: The software must exist.
  - DAL-D: High-Level Documentation/Tests
  - DAL-C: Low-Level Documentation/Unit Tests, Statement Coverage, and Code/Data Coupling Analysis
  - DAL-B: Branch Coverage
  - DAL-A: Source to Object Analysis and MC/DC Coverage
- DO-178 D-A closely related to ASIL A-D[1]

Example Applications

- DAL-E: Infotainment
  - Failure is a minor inconvenience
- DAL-D/C: Instruments
  - Failure can be mitigated by operator
- DAL-B/A: Engine Control
  - Failure could kill someone without warning

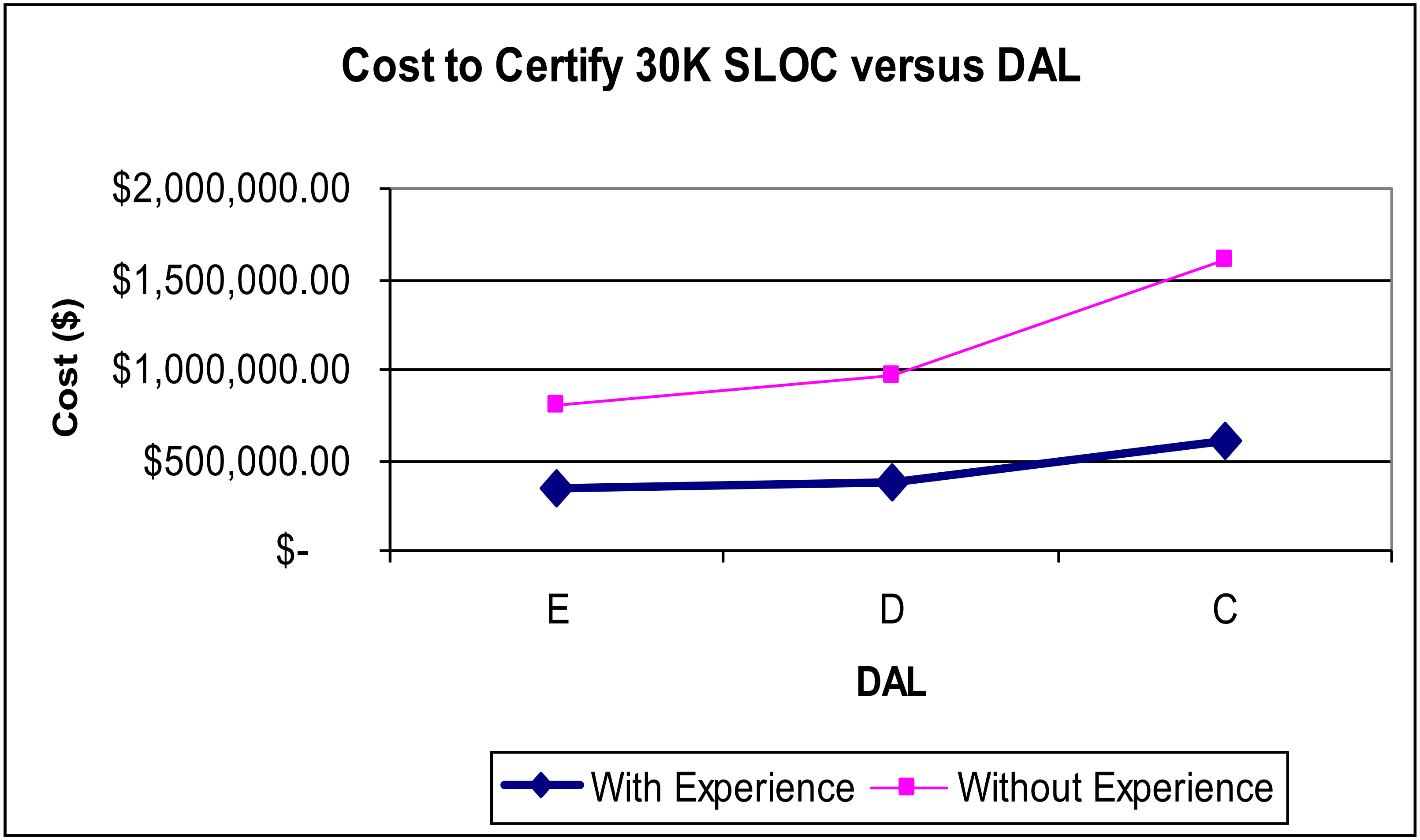
Certification Metrics[2]

- With Certification Experience
  - DAL-A: 0.67 hour / SLOC
  - DAL-B: 0.40 hour / SLOC
  - DAL-C: 0.20 hour / SLOC
  - DAL-D: 0.13 hour / SLOC
  - DAL-E: 0.11 hour / SLOC
- Without Certification Experience: Multiply by 3-4

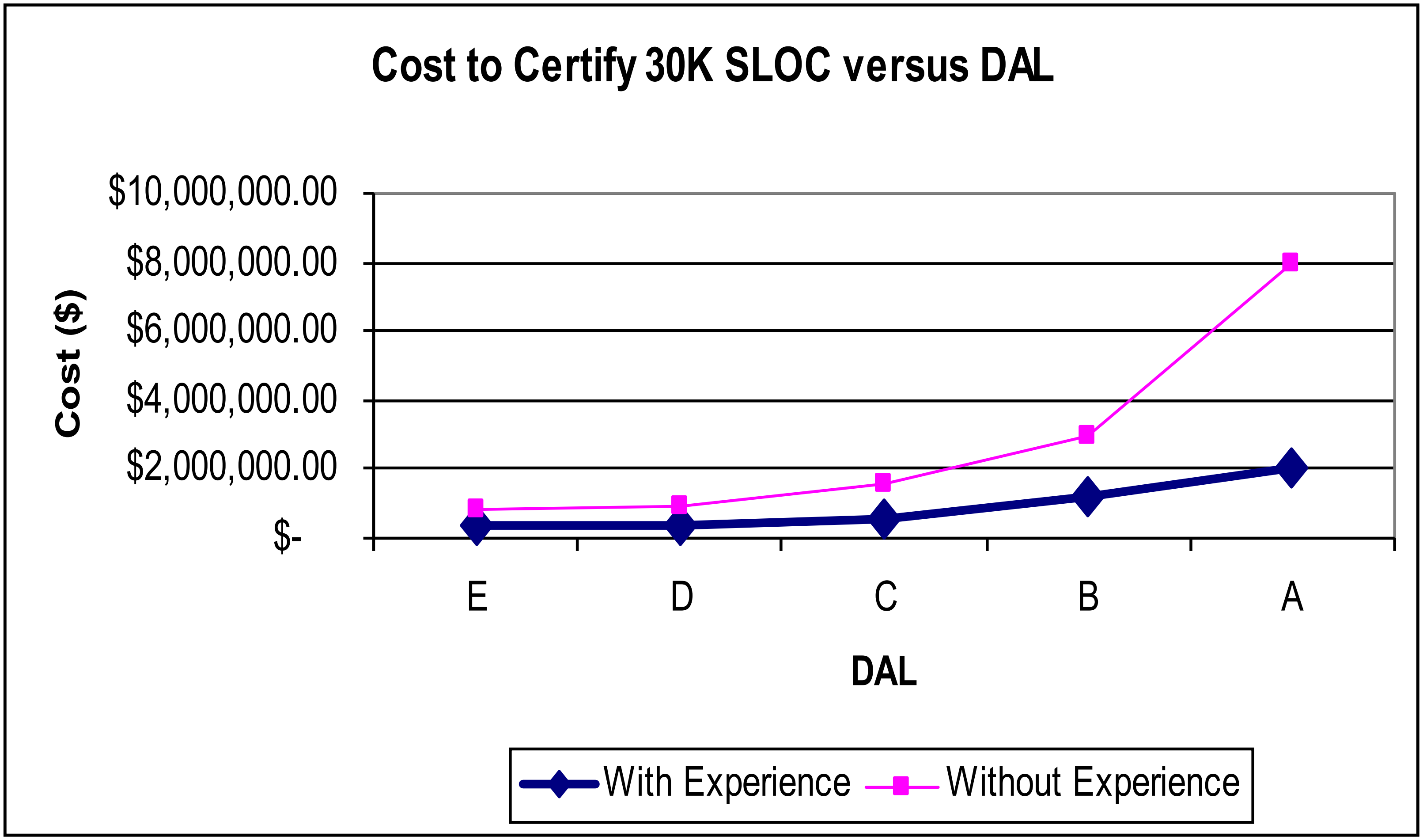
Certification Metrics In Pictures

- Rate: $100/hr
- Two Examples:
  - 30K SLOC: ~Xen ARM
  - 1 Million SLOC: Small Linux Kernel?

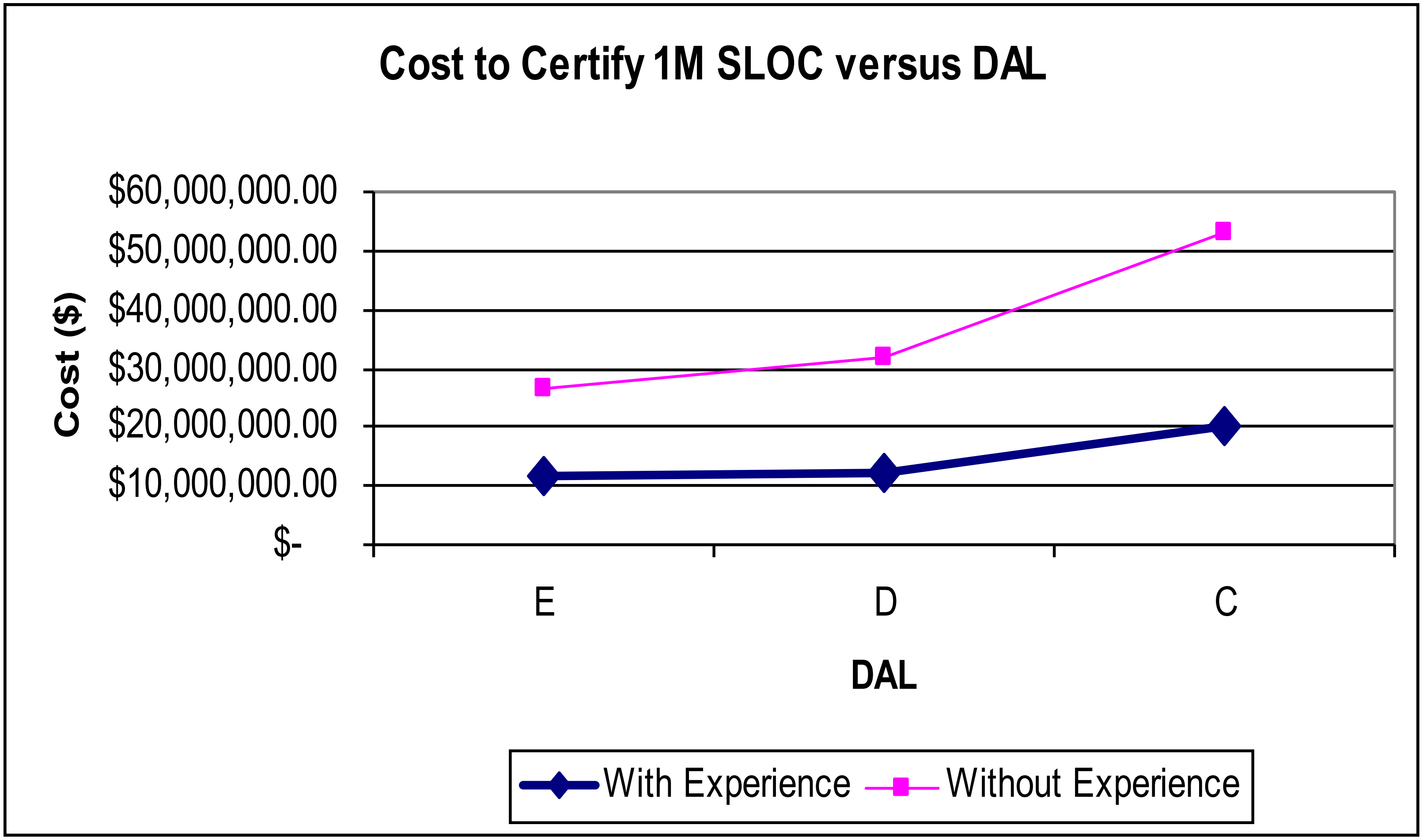
Example Certification Cost – 30K SLOC



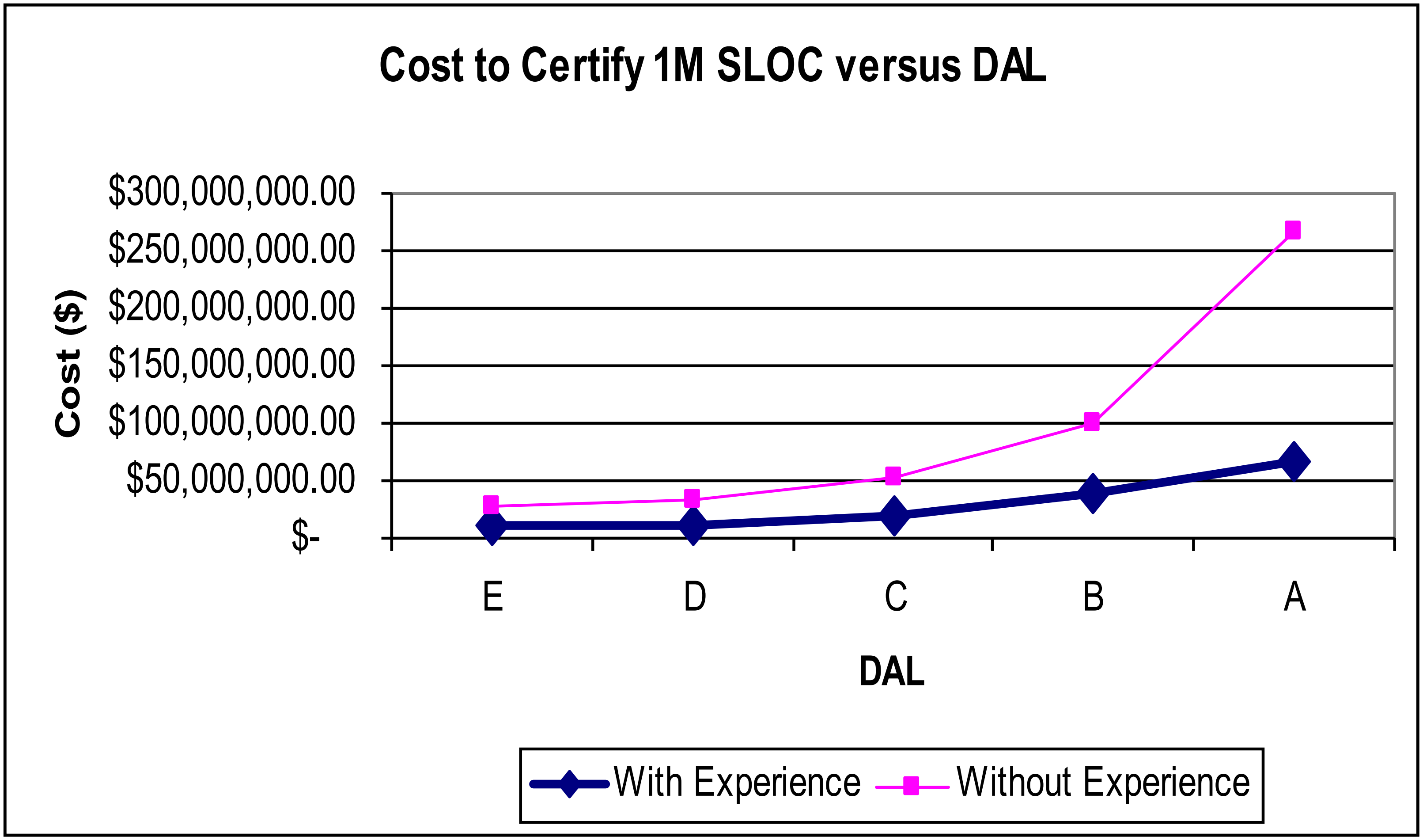
Example Certification Cost – 30K SLOC



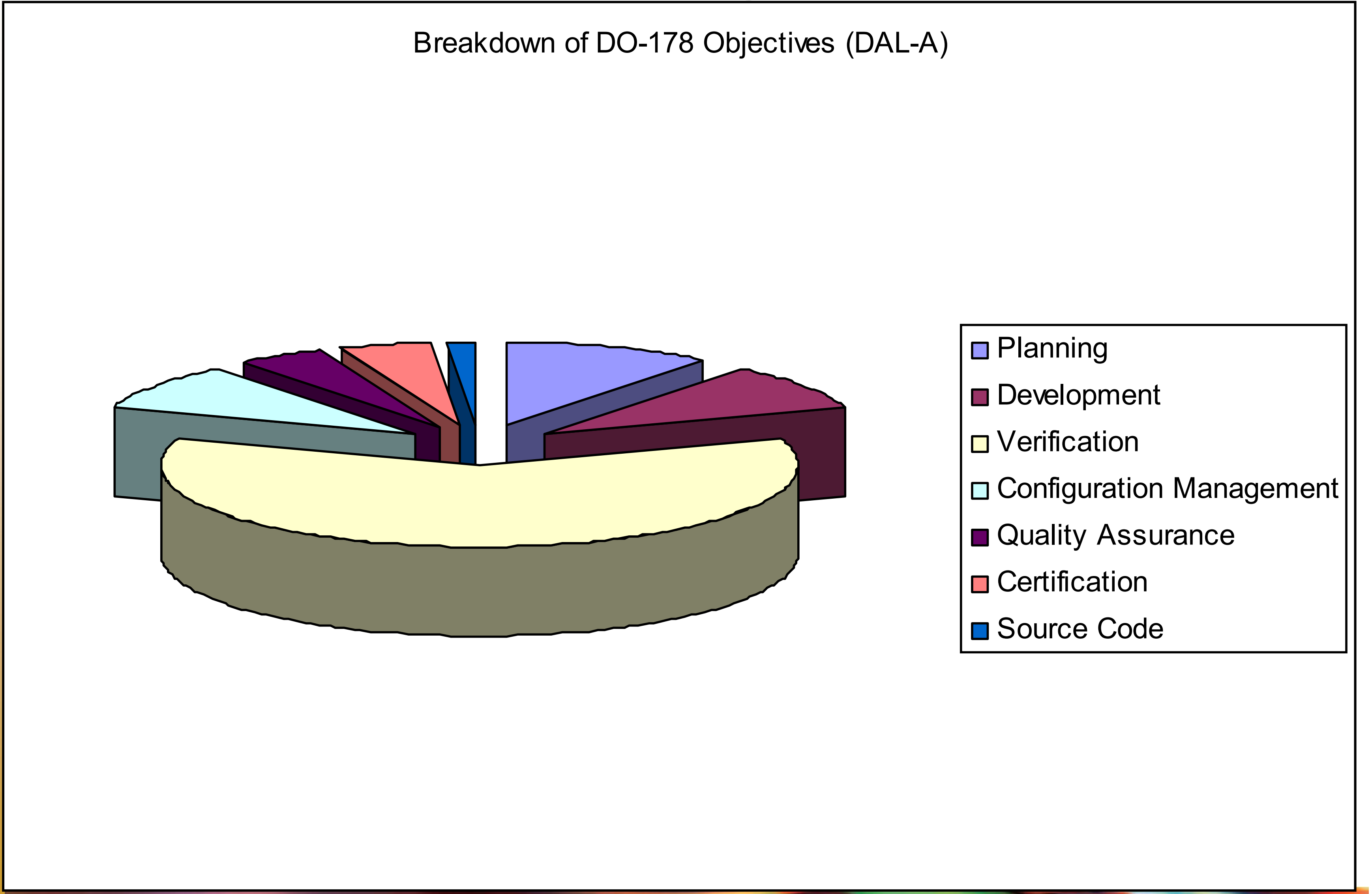
Example Certification Cost – 1M SLOC



Example Certification Cost – 1M SLOC



Where does the time go?



Overview

- DornerWorks Work
- Certification
- **Certifying Core Xen**
- Patch Example
- Beyond Core Xen
- Cost
- Conclusion
- Questions

General Xen Certification Plan

- Create a small subset
- Reverse Engineer Certification Artifacts for any extant features
- Forward Engineer any additional features

Xen Certification Guidelines

1. Create a small subset
2. Use virtualization extensions

Reverse Engineering – What can go wrong? [3]

- Poor reverse engineering justification
- Lack of a well defined Software Lifecycle Plan
- Abstraction and traceability problems
- No Access to original developers
- Complex and poorly documented source code

Commercial Aviation Safety Team (CAST)

Access to Original Developers

- “Developing the design, requirements, and test cases for a complex software component, such as an operating system, can be nearly impossible without some access to the original developers.” [3]

Xen Original Developers

- ARM
  - Ian Campbell
  - Ian Jackson
  - Stefano Stabellini
  - Julien Grall
- X86
  - Kier Frasier?
  - ???

Backup Plan

1. Git commit messages.
2. Archived Design Discussions on the mailing list.

Documentation and Comments

- “Many reverse engineering efforts start with source code that is complex and poorly documented. The code may contain numerous pointers and complex data structures. The code may also not contain commentary statements, which can make it difficult to understand.” [3]
- Reoccurring topic on Slashdot

Xen Certification Guidelines

1. Create a small subset
2. Use virtualization extensions
3. Focus on ARM

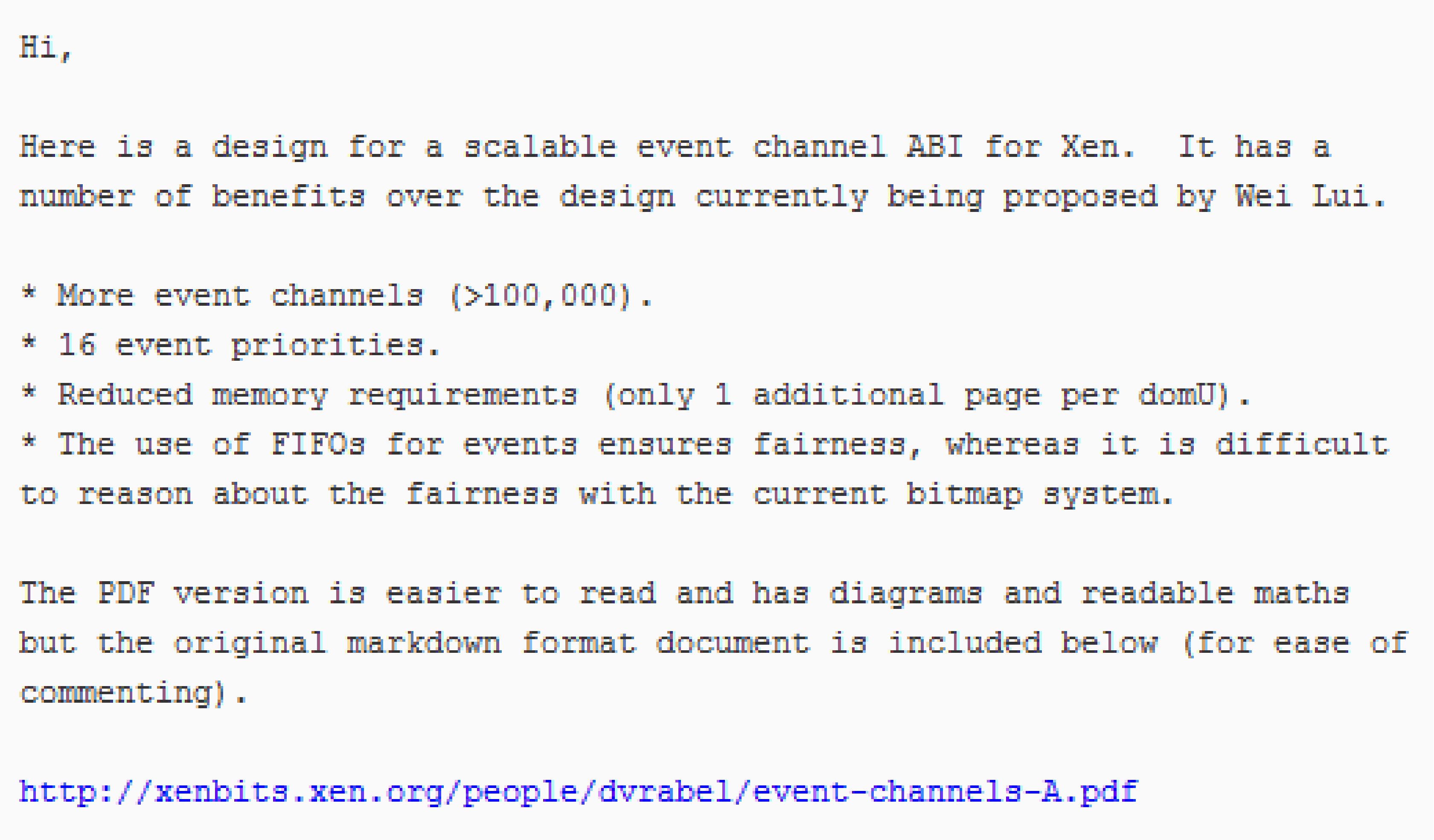
Overview

- DornerWorks Work
- Certification
- Certifying Core Xen
- **Patch Example**
- Beyond Core Xen
- Cost
- Conclusion
- Questions

Good Patch – Design Details

- David Vrabel – Scalable Event Channels

Design Details (DAL-E)



Hi,

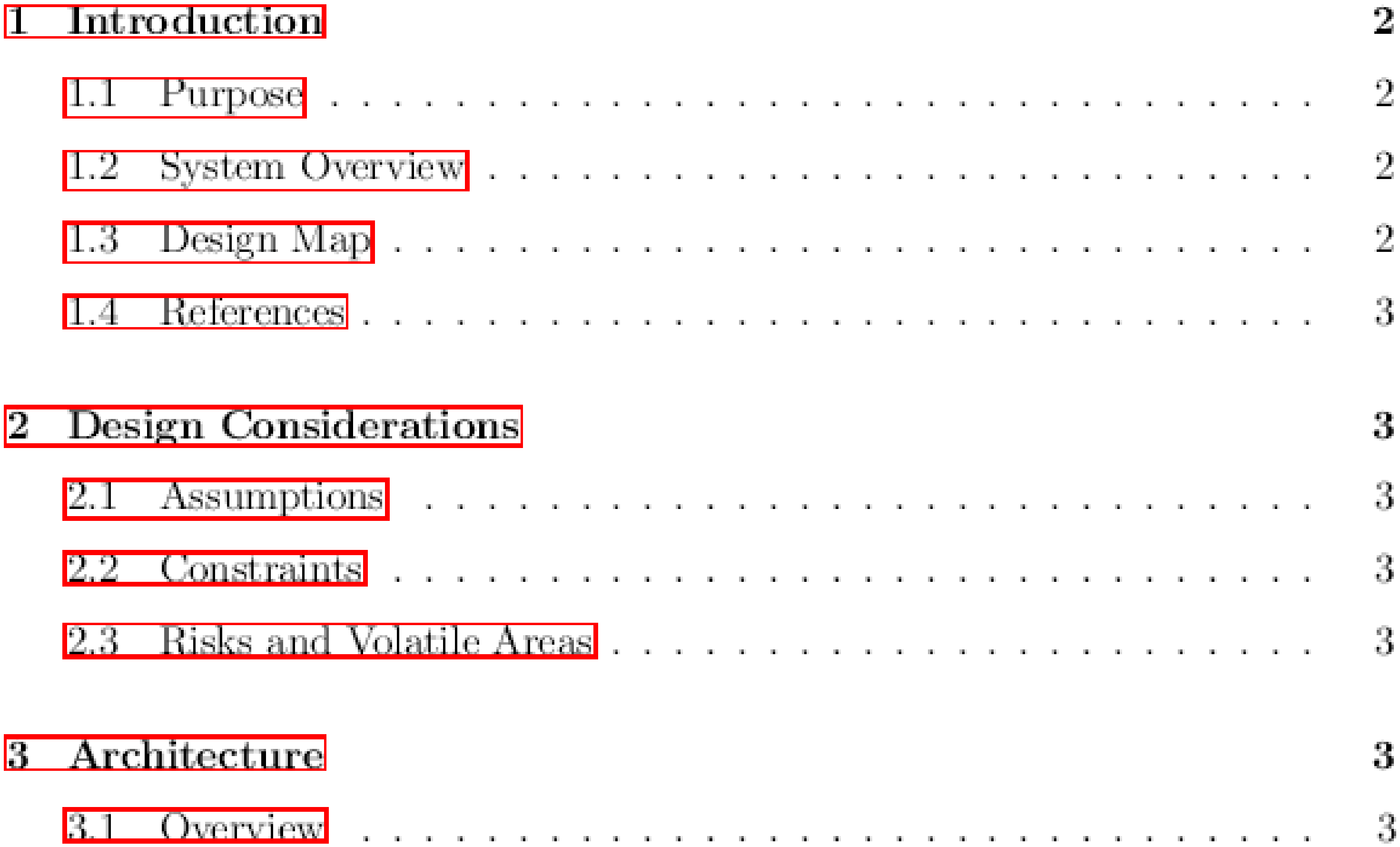
Here is a design for a scalable event channel ABI for Xen. It has a number of benefits over the design currently being proposed by Wei Lui.

* More event channels (>100,000).
* 16 event priorities.
* Reduced memory requirements (only 1 additional page per domU).
* The use of FIFOs for events ensures fairness, whereas it is difficult to reason about the fairness with the current bitmap system.

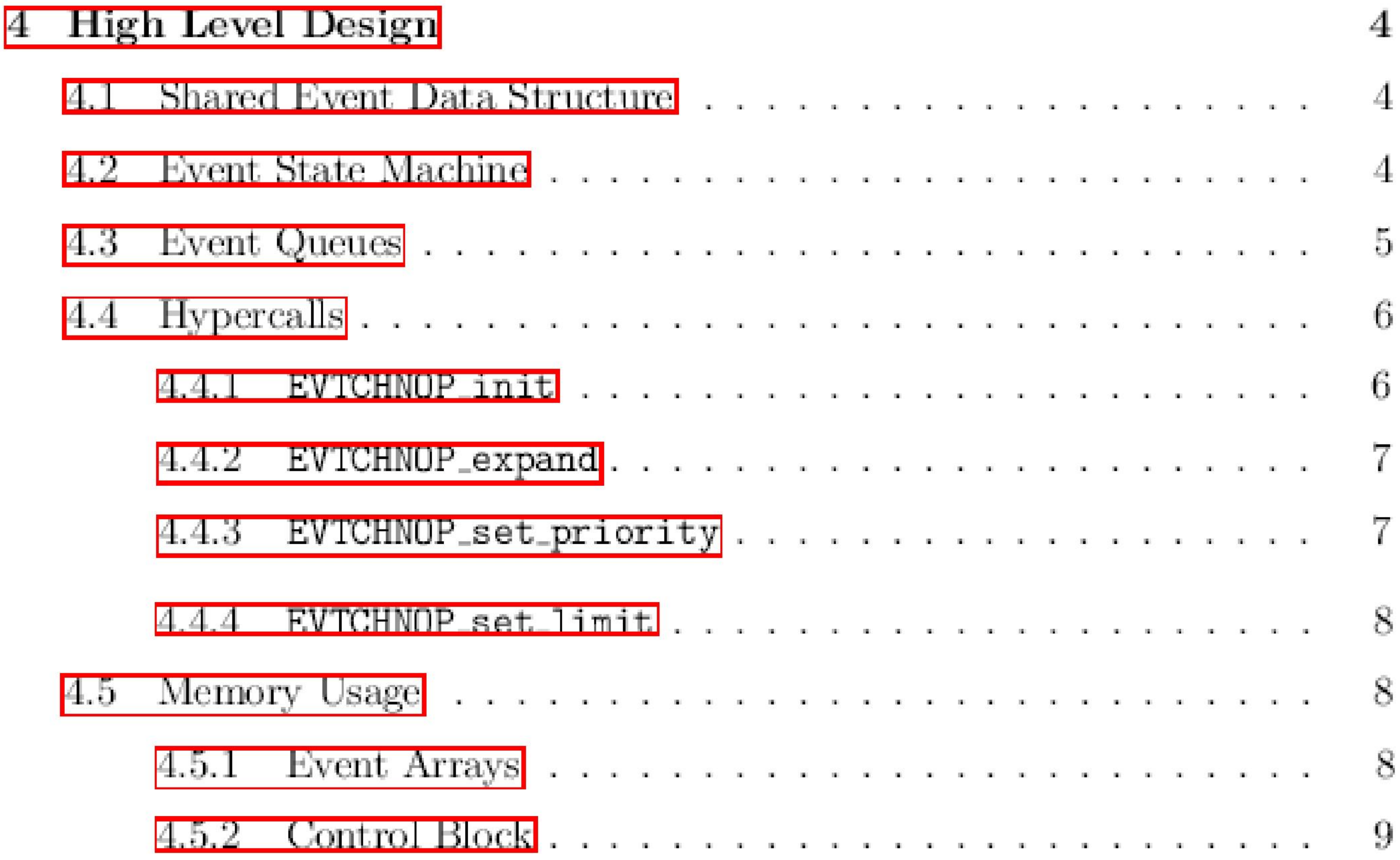
The PDF version is easier to read and has diagrams and readable maths but the original markdown format document is included below (for ease of commenting).

http://xenbits.xen.org/people/dvrabel/event-channels-A.pdf

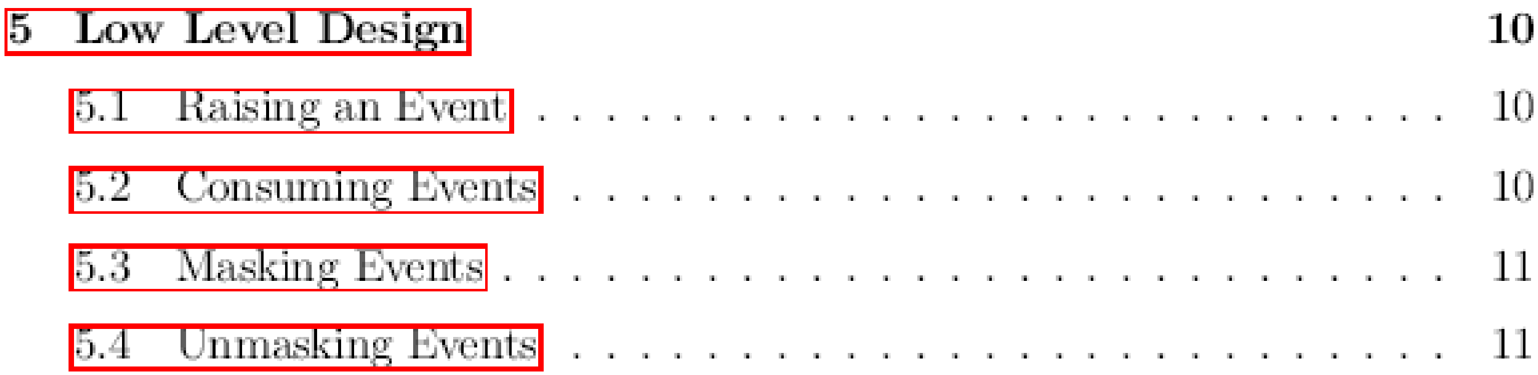
Design Details (DAL-D)



Design Details (DAL-D)



Design Details (DAL-C, B, A)



Overview

- DornerWorks Work
- Certification
- Certifying Xen
- Patch Example
- **Beyond Core Xen**
- Cost
- Conclusion
- Questions

Xen Helpers

- **U-boot or bootloader**
- Qemu
- XL and friends
- Dom0

Xen Certification Guidelines

1. Create a small subset
2. Use virtualization extensions
3. Focus on ARM
4. Create a simpler bootloader

Xen Helpers

- U-boot or bootloader
- **Qemu**
- XL and friends
- Dom0

Xen Certification Guidelines

1. Create a small subset
2. Use virtualization extensions
3. Focus on ARM
4. Create a simpler bootloader
5. Use direct pass-through or PV drivers

Xen Helpers

- U-boot or bootloader
- Qemu
- **XL and friends**
- Dom0

Xen Certification Guidelines

1. Create a small subset
2. Use virtualization extensions
3. Focus on ARM
4. Create a simpler bootloader
5. Use direct pass-through or PV drivers
6. <u>Create a simpler toolstack</u>

Xen Helpers

- U-boot or bootloader
- Qemu
- XL and friends
- **Dom0**

How hard is certifying Linux?

- It’s been done… to DAL-D.
- DAL-C is a big hurdle.
- It must be the “Rate of Change”, right?

Why such a big hurdle?

- DAL-D
  - High-Level Documentation
  - Functional Tests
- Information already exists.

Why such a big hurdle?

- DAL-C
  - Statement Coverage
  - Code/Data Coupling Analysis
  - Low-Level Documentation
  - Exhaustive Unit Tests
- Extremely unpopular tasks in the open source community.

Xen Certification Guidelines

1. Create a small subset
2. Use virtualization extensions
3. Focus on ARM
4. Create a simpler bootloader
5. Use direct pass-through or PV drivers
6. Create a simpler toolstack
7. Replace or Offload Linux dom0

Avoiding Linux – Open Source

- Mini-os dom0
- Custom dom0
- FreeRTOS?

Avoiding Linux - Other

- Already Certified dom0 (e.g. VxWorks, GreenHills, etc…)
  - HVM (or PVH) dom0
- Certified service domains
  - Still certifying a subset of Linux
- Unikernels

Overview

- DornerWorks Work
- Certification
- Certifying Core Xen
- Patch Example
- Beyond Core Xen
- **Cost**
- Conclusion
- Questions

Cost

- Certification Packages are expected to be expensive, but not that expensive
- Amortize certification costs, somehow
- Start with something less critical

Overview

- DornerWorks Work
- Certification
- Certifying Xen
- Patch Example
- Beyond Core Xen
- Cost
- **Conclusion**
- Questions

Conclusion

- Certification is a lot of work
- It needs to be done if a Xen guest is ever going to:
  - Fly a plane
  - Drive a Car
  - Perform Orthopedic Surgery
- The Xen developer community has a good frame work in place to make it happen

References

- [1] Matthias Gerlach and Stephan Weißleder, *Can Cars Fly? From Avionics to Automotive: Comparability of Domain Specifc Safety Standards*
- [2] *Certification Cost Estimates for Future Communication Radio Platforms*, 2009
- *[3] CAST-18: Reverse Engineering in Certification Projects*, 2003

Overview

- DornerWorks Work
- Certification
- Certifying Xen
- Patch Example
- Beyond Core Xen
- Cost
- Conclusion
- **Questions**

Questions

Contact Information

- Nathan Studer: nate.studer@gmail.com
- Robert VanVossen: robert.vanvossen@dornerworks.com