

STAR Critique meeting

Online and Offline
Computing

Jérôme Lauret

Micheal DePhillips, Wayne Betts,
Ernst Sichtermann

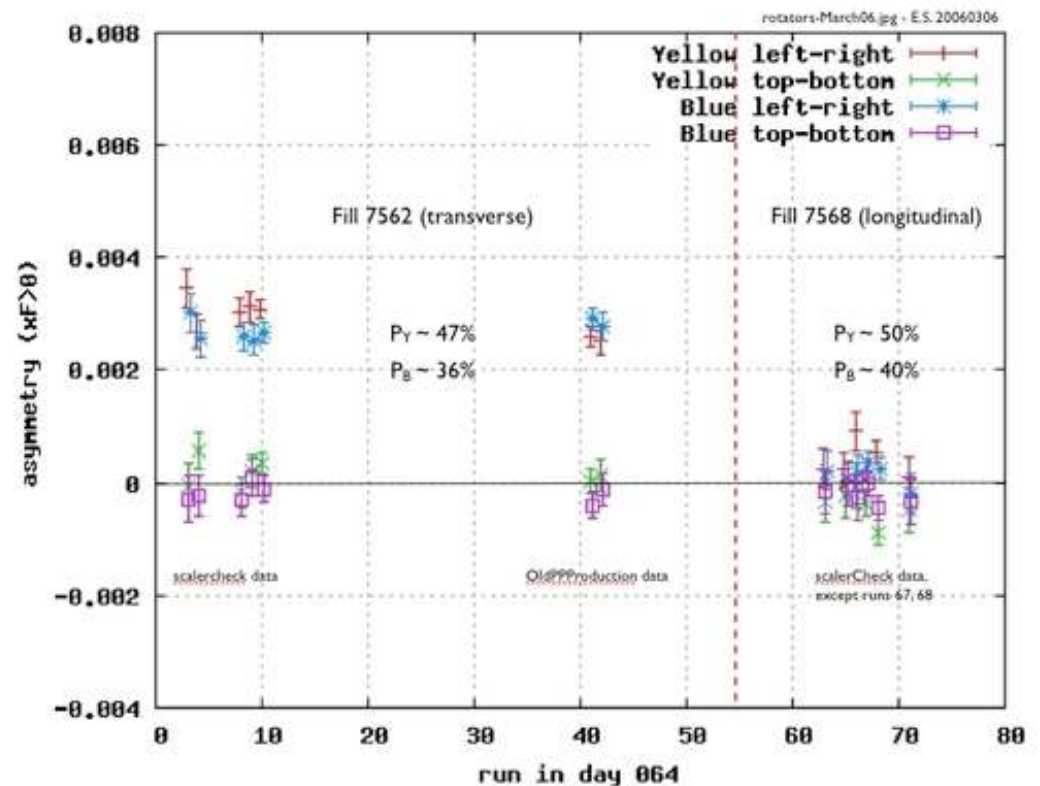


Topics coverage

- Scaler / trigger data and HPSS
- Db support online
- *Online QA (Sorensen and/or Laue plots ;-)*)
Overlap with DAQ, help from Valeri, etc ...
- *Offline QA*
- Shift signup
- Electronic shift log
- FastOffline
- Hardware configuration and Network layout

Scaler data and online

- Finally, we have the scaler files in HPSS (automatically that is)
- Past year back propagated
 - Ernst ...
- Future years
 - Need to migrate to CVS at BNL
 - Need full support as part of “QA”?
- **Opened question**
 - How many more like those?
 - i.e. need a re-evaluation of online tools used by spin-ers and multiple source of online QA



Some HPSS wilderness ...

- HPSS is NOT
 - A storage convenience for small files
 - A storage solution for any problems
 - Large amount of small files cut throughput by factor x2 at least
 - This is an and/or
- This year
 - Trigger files in HPSS
 - Several L2 offspring not accepted
 - Text files
 - Log files
 - Copies of data stream
- Need to re-discuss this and find solutions
 - This is a change of operation – many files, many sources ...
 - **Would benefit from central data movement mechanism**
 - **Will need mix solutions (for small files)**
 - Need efforts on user's side (is it __really__ needed??)

Db support online

- Database changes
 - Migration to Linux accomplished successfully
 - Need to complete migration and retire previous (Solrais)
- RunLog
 - Several extension, including reflecting trigger and scaler accounting
- Problems
 - Lost feed to Rich scalers – both times after an access – both times db Daemon lived on a appeared to be worked. Restarted of daemon fixed the problem.
 - Script was written to monitor and restart the daemon, deeper debug of code.
 - Event counts sometimes lagged
 - Cause: dbserver CPU throttled due to migration macro “stepping on its tail”, i.e. query accumulation
 - Happened only after a Magnet trip

Db support online

- Problems (continue)
 - A few times, online / offline migration issues
 - Impacted mostly FastOffline and “perception”
 - Added db migration as part of Offline QA shift
 - Problem sometimes related to overflow of data and external circumstances
 - Concerns
 - Some EPICS / information gathering and usage issues found this year
 - Never sure if data is gathered and the same data or something broke
 - Probably need “at the source” caching – archiver exists but ...
 - Need homogeneity of information
 - caGet versus caget ... but no source code
 - Initiated discussion with Mike Cherney
 - Jiro has (perhaps) good news - IRMIS

Shift Signup

- Not much to say ...
 - Well greased, solid tool
- Possible improvements
 - An early requirement mandated a check of non-overlapping shifts
 - This may be relaxed or modified
 - last minute over-commitment for shift coverage required trainees to be immediately in real shift slot
 - Could either relax the consideration for trainee/other position slots
 - Could add controls for Gurus (shift QA and shift coordinator) allowing “exception”

Electronic Shift Log

- Better used this year
- Novelties includes
 - Opening the tool to off-site access (point to point exception)
 - This is questionable in the long term due to Cyber Security issues (later topic)
 - Images limitation removed (large images never made in)
 - Only about a dozen attachment though (???!!)
 - Shift change-over form minor enhancements
- Problems
 - The confirmation of bad runs / good runs had a miss-feature
 - The window was not resizable, buttons where hidden
 - **FIXED**
 - The most frequent problem is a fatal error (frequent) problems with AJP13/JK2 Apache java handler
 - Could not upgrade during the run
 - This problem is present for the past 2 years at least ...
 - Frequency have increased to at least 4 times a day
 - Action items: upgrade to most recent version and re-assess
 - Access to database could freeze the GUI
 - Made thread safe and included timeout
 - Solution initially was considering a too short timeout

Miscellaneous

- FastOffline was at first on the verge of constant collapse
 - Several requests were conflicting
 - People waiting for A, slowed down by request B were un-happy
 - People on QA shift waiting for normal QA files un-happy
 - Had to put a foot down and disallow wild-wild west ...
 - Worked smoothly ever after ...
 - **Will produce procedure and scope document**
- Probably did worst in some area as per
 - “on call”
 - Lock of Shift Log reported but often fixed later
 - My cell did not ring once (probably lost ..)
 - Feedback online/offline better but still not as good as it could be
 - Data produced, QA ongoing but
 - people still asking about where it is, what are the results
 - **Need a procedure? Better integration ?**
 - **More cross-reference?**

Network and base line configuration

- The topic you are all dreaming to discuss ...
 - 8 AM to 11 AM meeting today was covering it ...
- As part of a DOE mandate to enhance CyberSecurity
 - Remediate all systems (including the one with exemptions)
 - Document enclave and describe purpose and scope
 - Document “controls” on that enclave
 - Make risk assessment
 - Note: MUST include protection from “inside” attack
- Strategy
 - Provide documentation
 - Inventoried all vulnerabilities and analyze situation
 - Fix what can be fixed and isolate what cannot

Network and base line configuration

Providing documentation

- Had about a week to deliver a document
 - Worked with Wayne/ Jack / Jeff
 - Made Wayne Betts the technical contact
 - Made myself (lucky me) as security contact (*happy to have anyone do this instead*)
- IMPORTANT: described the “system” as a two layer network
 - One layer is fire-walled
 - One “inner” layer is unroutable
 - You access the stark as usual
 - We MUST establish an internal controlled perimeter to the unroutable network
 - I propose to establish a gatekeeper model for that and reduce to a few machines
 - NOTE: all need to be documented
- This is a GOAL!! Some device are NOT protected
 - All device having “vulnerable” services (telnet interface, SNMP, ...)
 - Usually network power switches
 - The MUST be in the unroutable realm ...
- The question are:
 - is this acceptable?
 - If not, what are the arguments / cases / operational needs?

Feedback from System 1, CS

- A few comments were
 - What are the specific security needs of this major application
 - What are the physical security controls on the facility where the major application is located?
 - Does this facility have the same level of environmental controls (access control, fire protection, power protection...) as for the other major applications?
 - impact of unavailability of the major application ...
- Acceptable action item
 - document procedure i.e.
 - Shift sign-up, training, shift transitions
 - Explain code scope and usage
 - Explained this morning those are used for “QA”
 - This was well received ...

One more Cyber-c%#@#

- Several key nodes are considered vulnerable
 - Two of them, includes tpclaser
 - They MUST be brought to appropriate level
 - Explanation of software perhaps not running do not stand ground
 - If operational need, the node need isolation layer
- Other considerations
 - We have been struggling with multiple OS flavor on the Linux side (especially)
 - We need clear(er) documentation and tracking of access and changes
 - We need to
 - Homogeneous environment – easy maintenance
 - Reduce “flavor” of OS – intended to do so for this run, always get delayed
 - Reduce admin privileges (sorry!) and loosely managed systems
 - Node in – care of the S&C team and/or DAQ and/or trigger select-people