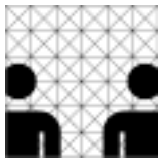
Universität Hamburg
Fachbereich Informatik

Arbeitsbereich
Angewandte Informatik
in Geistes- und
Naturwissenschaften (AGN)

Prof.Dr.Klaus Brunnstein
Vogt-Kölln-Straße 30
D-22527 Hamburg
Telefon+49 40 428 83 2406
Telefax+49 40 428 83 2226

brunnstein@informatik.uni-hamburg.de
http://agn-www.informatik.uni-hamburg.de/



Univ. Hamburg FB Informatik D-22527 Hamburg

An den Präsidenten
der Vereinigung Deutscher
Elektrizitätswerke - VDEW - e.V.
Herrn Dr. Heinz Klinger
c/o Frau Patricia Nicolai
Stresemannallee 23
D-60596 Frankfurt
FAX: 069 - 6304 - 289

=== Bitte sofort vorlegen! ===

Datum: 1999-12-18 (ISO-Norm-Darstellung für: 18. Dezember 1999)

Sehr geehrter Herr Dr. Klinger,

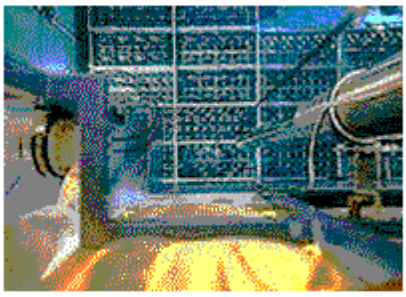
anlässlich des Gespräches in Ihrem Hause **zur Y2k-Notfallsicherheit der deutschen Elektrizitätswirtschaft**, zu dem ich von Frau Nicolai und Herrn Dr. Kienle eingeladen wurde, haben mir die Vertreter Ihres Verbandes, insbesondere Herr Dr. Höke (VGB und Preussen-Elektra) versichert, **dass im Sicherheitsbereich deutscher Kernkraftwerke nur festverdrahtete Schaltungen und keineswegs Computer- oder Mikroprozessor-gesteuerte Systeme eingesetzt** würden. Dies gelte auch für die AKWs Unterweser und Neckarwestheim, wo zwar **"digitale Leitsysteme" nachgerüstet** worden seien; diese lägen aber **ausserhalb des Sicherheitssystems** des Reaktors. Nachdem somit primäre Y2k-Wirkungen für den sicheren Reaktorbetrieb ausgeschlossen werden konnten, und weil bei einem Ausfall als Folge übersehener Y2k-Effekte bei den in sekundären und tertiären Bereichen eingesetzten Computersystemen die Notfallsicherheit durch den Rückgriff auf traditionelle, nichtinformatische Massnahmen beherrschbar ist, war ich zu dem Schluss gekommen, man sei hier "nach bester Praxis" vorgegangen. Dies entsprach auch meinen vorherigen Recherchen, und dieses habe ich bis dahin auch stets öffentlich vertreten (z.B. in der Sendung bei Frau Christiansen).

Bei einer **Nachprüfung** habe ich nun aber feststellen müssen, dass mir **offenkundig eine falsche Auskunft** gegeben wurde. Nach Analyse der Internetseite der Preussenelektra (die ich vorher nicht geprüft habe, weil mein PC-System das Laden der dort verwendeten sicherheits-gefährdenden JavaScripte verweigert, weil darüber bekanntlich einschlägige "Malware" verteilt werden kann!) finde ich dort nun **wesentliche Hinweise**, welche **die Aussagen Ihrer Fachleute in Zweifel zu ziehen geeignet** sind (und die sich darüber als ein Beispiel für bewusste Fehlinformation erweisen):

Auszug aus der aktuellen Seite der Preussen-Elektra vom 15. Dezember 1999:

Reaktorbegrenzungen

Neben dem Reaktorschutzsystem werden bei Druckwasserreaktoren sogenannte Begrenzungssysteme eingesetzt.



Diese haben die Aufgaben:

- Schutz des Reaktors vor unzulässigen Beanspruchungen beim Leistungsbetrieb
- Einhaltung der Betriebsparameter zur Absicherung von Störfallanalysen
- Vermeidung von Betriebstransienten mit Anforderung von Schutzaktionen

Diese Begrenzungseinrichtungen werden im wesentlichen nach den Anforderungen für Reaktorschutzsysteme ausgelegt und zählen zum Sicherheitssystem der Kernkraftwerke. Zum Errichtungszeitpunkt wurden diese Systeme ebenso wie die Reaktorschutzsysteme aus verdrahtungsprogrammierten Baugruppen ohne Mikroprozessoren aufgebaut.

Nach dieser Internet-Seite **gehören also die Begrenzungs-steuerungen zum Sicherheitssystem**; die hier verschwiegene Nachrüstung dieser Steuerung wird durch die Information der Reaktor-Sicherheitskommission (siehe: www.rskonline.de) bestätigt. Insofern ist die **Argumentation angeblich "festverdrahteter Schaltungen"** im Sicherheitsbereich für die baugleichen "digitalen Leitsysteme" der Firma Siemens (KWU) in den KKWs Unterweser und Neckarwestheim **nicht mehr haltbar** (ich ziehe dies weiterhin für die anderen deutschen AKWs nicht in Zweifel).

Erschwerend kommt der zweite (indirekte) Hinweis hinzu, dass nämlich **die Tatsache der Computer-Nachrüstung in sorgfältigster Formulierung ("Zum Errichtungszeitpunkt ...") der Öffentlichkeit verschwiegen** wird. Als ich diesen Aspekt mit Herrn Dr. Höke (der sich zu diesem Zeitpunkt im KKW Unterweser aufhielt) besprechen wollte, wurde mir nach einigen Stunden von einer Mitarbeiterin ausgerichtet, er sei in Absprache mit einer "Frau Dr. Uhlmann" (die mir weder vom Namen noch der Position bekannt war) nicht zu einem Gespräch bereit.

Einmal abgesehen von der **Frage**, ob ein **KKW-Betreiber, der solche Informationen der Öffentlich verschweigt bzw. die Öffentlichkeit irreführt**, für sich das Attribut **"zuverlässig"** in Anspruch nehmen kann, ist bei dieser Sachlage **nicht mit der notwendigen Sicherheit auszuschliessen**, dass es infolge primärer Auswirkungen eventuell **übersehener Y2k-Wirkungen** der sog. "digitalen Leitrechner" **zu Beeinträchtigungen der Sicherheit beider Reaktoren kommen kann**. Mir ist noch zur Genüge in Erinnerung, wie ein angeblich sicheres Betriebssystem aus dem Hause Siemens (welches einen lange Zeit unerkannten schwerwiegenden Programmierfehler enthielt) zu einem mehrtägigen Stillstand eines "sicheren Bahnbetriebssystems" führte. Obwohl jener Vorfall glimflich ablief (hier konnten "nur" drei Tage lang keine Züge fahren), sind **schwerwiegende Folgen derartiger eventuell übersehener Fehler nicht a priori**

auszuschliessen. Und die Erkennung solcher Fehler bedarf spezieller Kenntnisse, die nach meiner Überzeugung bei den Überprüfungen nicht vorhanden waren. Selbst für die Annahme, dass die "traditionellen Sicherheitsmassnahmen" bei einem Y2k-induzierten Ausfall im Sicherheitssystem zuverlässig greifen würden, liegen mir keinerlei Hinweise vor.

Hier macht sich nun störend bemerkbar, dass **die deutsche Reaktorwirtschaft** - auch bedingt durch die unvertretbar späte Aufforderung des für Reaktorsicherheit zuständigen Bundesministeriums (siehe "weitergeleitete Nachricht " 04/98 mit Kriterienkatalog 04/98a) - **allzu spät erst im 2. Halbjahr 1998 mit der Überprüfung der Kernkraftwerke begonnen hat** (in USA und England wurden solche Projekte spätestens 1997 begonnen, wie die Dokumentationen beweisen). Anders als in England und den Vereinigten Staaten **fehlen hierzulande auch Fachleute mit hinreichendem Informatik-Know-How** in diesem hochsicherheitsbedürftigen Anwendungsgebiet (dies war auch Gegenstand des Gespräches in Ihrem Hause).

Unter diesen Umständen halte ich es für **dringend geboten**, die erwähnten **digitalen Leitsysteme von einem unabhängigen Fachmann überprüfen zu lassen**; ein solcher kann nach Sachlage nur aus den USA oder England kommen. Soweit dies nicht mehr rechtzeitig zu einem schlüssigen Bild (welches die in dieser Sachlage nicht ausreichend fachkundig besetzte RSK auch nicht "abnicken" kann) kommt, halte ich es **aus verantwortlicher Vorsorge für unausweislich, die beiden Kernkraftwerke über das Jahresende abzuschalten** (wogegen m.W. auch kein Mangel an elektrischer Leistung spricht).

Mit freundlichen Grüssen

(Prof. Dr. Klaus Brunnstein)