KKK Arbeits - Bericht

TKEK	1529	2007
Nummerierung	(AKZ lfd. Nr.	Jahr)

Thema/Anlass

Verhalten des Prozessrechners beim Ereignis N01/07 „Reaktorschnellabschaltung durch kurzzeitigen Ausfall der Eigenbedarfsversorgung aufgrund Kurzschluss in einem Maschinentrafo“

12.07.2007	
Datum	Revision

Verfasser	AKZ	Tel.

Unterschrift Freigebender

Zusammenfassung Textseiten 4 Anlagen 1

Zusammenfassung:

Durch ein sehr stark erhöhtes Signalaufkommen und einer für diese Situation nicht ausreichende Prioritätenverteilung im Betriebssystem, ist eine nicht notwendige Umschaltung der Prozessrechner erzwungen worden.

Durch diese nicht zeitlos durchführbare Umschaltung ist es zum Verlust von aktuellen Zeitstempeln gekommen, die durch Ersatzzeiten bei einer Generalabfrage ergänzt wurden. Daher ist eine zeitfolgerichtige Signalverfolgung nach der Rechnerumschaltung für eine bestimmt Zeit nur eingeschränkt möglich.

Zu jedem Zeitpunkt wurden alle Signale erfasst und in der Warte auf den Bildschirmen angezeigt. Einige wenige Signalwechsel wurden nicht archiviert.

Die Abhilfemaßnahmen zur Verbesserung des Rechnerverhaltens bei derartigen Anlagenverhältnissen werden aufgezeigt und sollen in der 29. KW umgesetzt werden.

Unterschrift / Verfasser

Verteiler (falls nur Zusammenfassung zur Kenntnisnahme: "z.K" anfügen):

Verteiler (intern):

UI-Ident-Nr.: **02070055447 /0017**

Sachverhalt:

In dieser Darstellung werden die Abläufe und Funktionen des Prozessrechners erklärt, die während des Ereignisses vom 28.06.2007 im KKW Krümmel benötigt wurden.

Der Prozessrechner befand sich in folgendem Zustand:

Der Rechner JW10 (VP001) war Master und der Rechner JW20 (VP002) war Slave. Beide Rechner liefen störungsfrei seit der letzten Datensicherung. Alle Drucker und Bildschirme waren normal in Betrieb, Anzeigen von Supervisor und MVP waren aufgeschaltet, einige Bildschirme zeigten Trends. In der Warte wurde die Anlage normal genutzt.

Ereigniseintritt:

Gegen 15:02 Uhr trat das Ereignis in der Anlage ein. Zu diesem Zeitpunkt entstand durch die vermehrten Schalthandlungen ein Meldeschwall in der Prozessrechneranlage. Alle Erfassungsrechner arbeiteten ohne Fehler.
Auch das erhöhte Meldungsaufkommen (ca. 3400 Meldungen in den ersten drei Sekunden) bedeutete keine Funktionsbeeinträchtigung auf der Erfassungsebene.

Der Verarbeitungsrechner JW10 begann zeitnah diese Daten bei den Erfassungsrechnern abzuholen und in zwei Tabellen (PLS_Bin_History und PLS_Ana_History) abzulegen. Aus dieser so genannten Kurzzeithistorie werden die Anzeigen in der Warte gespeist.
In einem späteren Zyklus (max. Verzögerung bis zu 20 Sek.) werden die Daten auch in das Langzeit Archiv (Historien) geschrieben. Diese Verzögerung wird benötigt, um verspätete Meldungen noch zeitfolgerichtig einzusortieren.

Parallel dazu wird ein Abgleich zwischen den beiden Maschinen (Master/Slave) durchgeführt. Der Master gibt seine Daten mit einer zeitlichen Verzögerung (ca. 1 Sek.) über eine separate Leitung an den Slave weiter. Automatisch ausgelöste Protokolle und Auswertungen werden aus dem Langzeit Archiv erstellt. Wird so eine Abfrage ausgelöst und die benötigten Daten sind noch nicht im Archiv, so wird diese Abfrage mehrfach wiederholt. D.h. das Archiv wird zusätzlich beschäftigt, was normalerweise kein Problem bedeutet.

Alle diese Funktionen (einlesen, anzeigen, archivieren, synchronisieren und auswerten) sind prioritätsgesteuert.

Zum Zeitpunkt des Meldeschwalls hat der Archivprozess versucht Daten auf seine Festplatte zu schreiben und ebenfalls Daten für gerade angeforderte Protokolle zur Verfügung zu stellen. Um diese Anforderungen erfüllen zu können, benötigte das Archiv mehr Ressourcen (CPU und Speicher) von dem Betriebssystem VMS.

Da die anderen Prozesse (einlesen, synchronisieren, anzeigen) eine höhere Priorität haben, hat das Betriebssystem dem Archiv keine weiteren Ressourcen gegeben. Dadurch hat der Archivprozess RTHistServer seine Tätigkeiten eingestellt und dem Zentralsystem (RTA) über ein Important Flag gemeldet, dass er nicht mehr arbeiten kann. Dieses Flag sagt aus, dass der Master Prozessrechner nicht mehr komplett arbeitet und eine Umschaltung notwendig ist. Diese Umschaltung wurde nun eingeleitet, da ein Reservesystem zur Verfügung stand. Damit wird das alte Mastersystem gestoppt und alle Tabellen aus dem Speicher gelöscht, da nicht mehr sichergestellt ist, dass diese noch aktuell sind. Die Daten, die noch auf dem Wege in das Archiv waren, werden noch in eine CSV Datei geschrieben und gehen somit nicht verloren.

Der Slave Rechner fängt nun an, die Funktion des Masters zu übernehmen. Dafür kontrolliert das neue Zentralsystem RTA die ihm noch bekannten Zustände (Prozessabbild) der Anlage. Er macht eine Generalabfrage an alle Erfassungsrechner, um sein Prozessabbild zu aktualisieren. Dabei stellte der neue Masterrechner (VP002) fest, dass einige seiner bekannten Zustände aus dem Kurzzeitarchiv mit dem Anlagenzustand nicht übereinstimmen. Da der alte Master diese Zustände schon ausgelesen und nur zum Teil bearbeitet, aber noch nicht synchronisiert hatte, gab es Unterschiede zwischen beiden Rechnern.

Diese Daten wurden nun neu eingelesen und mit einem neuen Zeitstempel versehen. Den Zeitstempel der tatsächlichen Änderung hatte nur der alte Master eingelesen. Der Erfassungsrechner löscht diesen Zeitstempel, wenn er einmal seine Daten dem Verarbeitungsrechner zur Verfügung gestellt hat. Damit wird sichergestellt, dass Daten nicht doppelt oder dreifach zu einem späteren Zeitpunkt eingelesen werden. Somit kann bei einer Generalabfrage auch nur der Zeitpunkt als neuer Zeitstempel genutzt werden, der bei der Abfrage aktuell ist.

Im normalen Betrieb macht das auch kaum einen Unterschied, allerdings in der Situation eines Meldeschwalls können zeitliche Verschiebungen entstehen.

Nach dieser internen Bereinigung (ca. 15:03:30 Uhr) hat der VP002 (JW20) den Betrieb des Masters komplett übernommen und weiter fehlerfrei gearbeitet.

Am Montag, den 02.07.2007 wurden dann die CSV Dateien in das bestehende Langzeit Archiv nachgeladen und stehen seither auch zur Verfügung. Nach bisherigen Erkenntnissen fehlen einige wenige Signalwechsel.

Fazit:

Durch ein sehr stark erhöhtes Signalaufkommen und einer für diese Situation nicht ausreichende Prioritätenverteilung im Betriebssystem ist eine nicht notwendige Umschaltung der Prozessrechner erzwungen worden.

Durch diese nicht zeitlos durchführbare Umschaltung ist es zum Verlust von aktuellen Zeitstempeln gekommen, die durch Ersatzzeiten bei einer Generalabfrage ergänzt wurden. Daher ist eine zeitfolgerichtige Signalverfolgung nach der Rechnerumschaltung für eine bestimmt Zeit nur eingeschränkt möglich.

Zu jedem Zeitpunkt wurden alle Signale erfasst und in der Warte auf den Bildschirmen angezeigt. Einige wenige Signalwechsel wurden nicht archiviert.

Das Meldeschwallvolumen hat mittlerweile durch Nachrüstungen in der Anlage die Spezifikation der IBS von 2001 überschritten, wodurch mehrere Parameter nicht mehr aktuelle Basisbewertungen hatten.

Abhilfemaßnahmen:

- der Umschaltvorgang wird mit neuen Parametern optimiert
- die I/O Buffer werden um 50% vergrößert
- Recoveryzeit für I/O Verarbeitung wird rückgreifend verlängert
- Protokolle und Abfragen auf das Archiv werden optimiert und zeitlich verzögert
- Test des Meldeschwalls inkl. einer Umschaltung mit Hilfe eines Meldeschwall-Generators

Anlage: Struktur der Prozessrechneranlage

Struktur der Prozessrechneranlage