Appears in Working Notes of the AAAI Spring Symposium on
Human Interaction with Autonomous Systems in Complex Environments
p. 113-116, Stanford, CA, March 2003

Plant + Control System + Human: Three's a Crowd

(Extended Abstract)

Kurt D. Krebsbach
Department of Computer Science
Lawrence University
Appleton, WI 54911
kurt.krebsbach@lawrence.edu

David J. Musliner
Honeywell Technology Center
3660 Technology Drive
Minneapolis, MN 55418
david.musliner@honeywell.com

Introduction

We contend that current approaches to supervisory control of complex systems are inherently insufficient. In this paper, we provide a collection of anecdotal evidence supporting this contention, and claim that combining innate human flaws with sophisticated but brittle automation leads to a slew of problems. We briefly outline future research directions that we believe will lead to more robust, capable, and efficient autonomous control systems that team effectively with humans. In short, while improved human interaction systems can help, the fundamental change required is the addition of another partner in control, a model-based intelligent system that can turn "three's a crowd" into "four's a team."

The anecdotes and scenarios described below have all happened, many during our visits to petroleum refineries and chemical plants around the country.

Background: Refineries and Control

Petrochemical refining is one of the largest industrial enterprises worldwide. The functional heart of a refinery, and the most economically critical component, is the Fluidized Catalytic Cracking Unit (FCCU). As illustrated in Figure 1, the FCCU is primarily responsible for converting crude oil (feed) into more useful products such as gasoline, kerosene, and butane (Leffler 1985). The FCCU *cracks* the crude's long hydrocarbon molecular chains into shorter chains by combining the feed with a catalyst at carefully controlled temperatures and pressures in the riser and reactor vessels. The resulting shorter chains are then sent downstream for separation into products in the fractionator (not shown). The catalyst is sent through the stripper and regenerator to burn off excess coke, and is then reused.

Figure 2 illustrates how a typical state-of-the-art refinery is controlled. The Distributed Control System (DCS) is a large-scale programmable controller tied to plant sensors (e.g., flow sensors, temperature sensors), plant actuators (e.g., valves), and a graphical user interface. The DCS implements thousands of simple control loops (e.g., PID loops) to make control moves

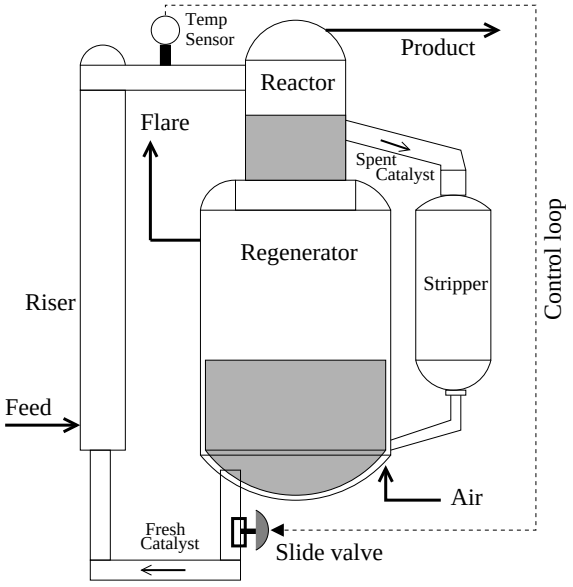

Figure 1: A Fluidized Catalytic Cracking Unit.

based on discrepancies between setpoints and present values. For example, as depicted in Figure 1, the dotted line connecting the temperature sensor and the riser slide valve denotes that the position of the slide valve is dependent on the temperature being sensed in the riser. As the temperature drops, the slide valve will be opened to increase the flow of hot catalyst. A typical FCCU will have on the order of one thousand readable "points" (sensors), and a few hundred writable "points" (actuators). In addition to PID control loops, the DCS can be programmed with numerous "alarms" that alert the human operator when certain constraints are violated (e.g., min/max values, rate limits). "Advanced control" is the industry term for more powerful mathematical control techniques (e.g., multivariate linear models) used to optimize control parameters during normal operations.

The human operators supervise the operation of the highly-automated plant. This supervisory activity includes monitoring plant status, adjusting control parameters, executing pre-planned operational activities (e.g., shutting down a compressor for maintenance),

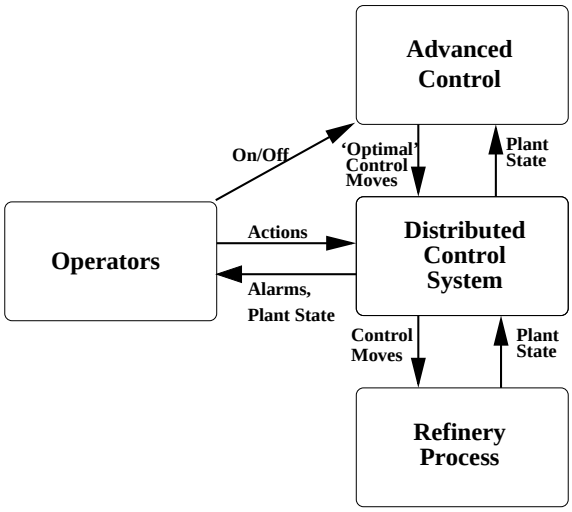

Figure 2: State-of-the-Art Refinery Control.

and detecting, diagnosing, compensating for, and correcting abnormal situations. The operator has a view of the values of all control points, plus any alarms that have been generated. The actions the operator is allowed to take include changing setpoints, manually asserting output values for control points, and toggling advanced control modules.

Abnormal Situations

Abnormal situations occur frequently in refineries, and violate many of the assumptions on which the DCS control systems are designed. Minor incidents often cause dozens of alarms to trigger, requiring the operator to perform anywhere from a single action to dozens, or even hundreds, of compensatory actions over several hours. Major incidents can precipitate an *alarm flood*, in which hundreds of alarms trigger in a few seconds, leading to scrolling lists of alarm messages, panels full of red lights, and insistent klaxons. In these situations, the operator is faced with severe information overload, which often leads to incorrect diagnoses, inappropriate actions, and major disruptions to plant operations. Abnormal situations can be extremely costly, resulting in poor product quality, schedule delays, equipment damage, reduced occupational safety, and environmental hazards.

Because abnormal situations are so serious, many regulatory and administrative structures are already in place to help manage them. Primarily, operators are trained to respond to abnormal situations based on extensive Standard Operating Procedures (SOPs) that are written down. The procedures can be quite long (dozens of pages), with lots of logical control structure and contingencies, since the exact state of the plant is almost never known with certainty. Many procedures involve sampling data, confirming other readings, performing diagnostic tests, conferring with other plant personnel, and adjusting DCS control parameters. Some procedures apply to extremely general contexts (e.g., we're losing air pressure from somewhere), while some are less general (air compressor AC-3 has shut down), and some are very specific (the lube oil pump for AC-3 has a broken driveshaft).

While visiting more than five refineries and recording operations during more than a week of formal observation time, we encountered numerous incidents showing the instability and brittleness of the current approach to mixed-initiative supervisory control.

Stupid Human Tricks

The foibles and faults of humans are well-known and well-documented. However, it is instructive to examine a few of the refinery incidents we observed to illustrate the scope and import of human fallibility.

Simple Mistakes

The DCS is controlled from a broad keypad with which the operator calls up various data displays and enters new setpoints for different PID control loops. The operators become extremely adept at using these keypads, and perform navigation and data entry very quickly. Interestingly, the DCS has essentially no idea what its control loops are actually doing. Thus it has no idea that changing a valve from 5% open to 99% open in one step is a bad idea. Thus when the operator accidentally enters "99" instead of "9" and hits "enter" before noticing the problem, the DCS happily obeys the command. Even if the operator instantly recognizes the mistake and enters the correct command as quickly as possible, the valve will have moved, and hundreds of pounds of extra material will have flowed past the valve. This type of simple mistake can introduce a disruption in plant operations that lasts for hours, producing off-spec products and costing tens or hundreds of thousands of dollars.

Cultural Complications

At a higher level, humans also perform suboptimally due to socio/cultural influences. For example, a plant operator may overestimate his expertise and understanding of a complex plant unit, and disregard the operational procedures manuals. Although most plant procedures are written to comply with government agency regulations (e.g., OSHA), they are usually written once in very general terms and are seldom revised. Operators consider these procedures little more than "general guidelines." The interpretation and execution of a given procedure by different operators can vary widely. However, the procedures are developed by the engineers who design and install the plant, as well as

the most senior operators. The average operator tends to have a much coarser mental model of how the plant actually works.

As a result, while a written procedure may specify that a valve be closed slowly and incrementally, over a period of half an hour, one operator may conclude that the instruction is too annoying, requiring him to watch the clock and make dozens of entries on the control board. So, understanding that the eventual result is a closed valve, the operator may instead close the valve in two large increments spaced a few minutes apart. Part of the fault here lies in hubris, and part lies in the lack of explanations and rationale to back up sterile procedure specifications. Hours later, after finally stabilizing the plant process and restoring efficient operations, the operator may not even recognize that this disruption was solely due to ignoring established procedures.

Even worse, he may never get any negative feedback from peers, superiors, or training personnel. We repeatedly observed this type of procedural error and had detailed discussions with an operator trainer who also observed and recorded these mistakes. In all cases, the trainer indicated he would not discuss the incident with the operator. Why not? To avoid offending or angering him. How then would the operator improve? The trainer might discuss the subject procedure during a general review session, but would not point out mistakes.

Stupid Automation Tricks

Criticisms of automation and technology abound. Below, we provide two examples that are somewhat more interesting than the "blinking VCR clock."

The Foolie

Consider again the FCCU in Figure 1. Recall that the position of the slide valve (bottom) is dependent on the temperature being sensed in the riser. This feedback control loop is designed to keep the reaction in the riser burning within the desired temperature range, by regulating the amount of catalyst. As the temperature drops, the slide valve will be opened to increase the flow of hot catalyst. The increase in hot catalyst will cause the reaction in the riser to burn hotter, raising the temperature at the temp sensor point, eventually causing the slide valve to remain steady or begin to close.

It is important to note that this control loop's default behavior depends on the *implicit* assumption that the air supply remains constant, and that the catalyst-to-air ratio can be regulated by adding or subtracting catalyst alone.

However, in one abnormal situation we studied, half of the required combustion air ("Air" in the diagram) is lost due to a malfunctioning blower. In this situation, the reduced oxygen level will also cause a temperature drop in the riser, but because the control loop does not have any knowledge of air flow, its response will be exactly the wrong one. Adding more catalyst with half the air will further upset the catalyst-to-air balance, and will *decrease* the riser temperature.

The only option available to the operator in this case (and the one that was recommended in the official plant procedure) is to adjust the setpoint on the temperature controller to an abnormally low value, thus "fooling the controller" into thinking that the situation is normal, so that it will not add more catalyst.

Generalizing from this example, we see a whole class of problems in which the simple DCS controllers perform inappropriate actions during abnormal situations, because their underlying (implicit) assumptions are violated. And, because the DCS does not check these assumptions, the human must have a mental model of both the plant *and the controller.* Using this controller model, the human must anticipate inappropriate actions and use the inputs he does control to fool the controller into either doing the right thing or at least not making things worse.

Bailing Out

During normal operation, advanced process control (APC) software can be used to autonomously control parameters of the plant to keep it running at near-peak profitability. However, APC is currently an all-or-nothing proposition; if it is on, the operator does not participate in the functions it is controlling, and if it is off, the operator is completely in charge of all aspects of the unit. For this reason, advanced control techniques quickly become inappropriate during abnormal situations, and the controller is typically turned off. Then human personnel, including board operators, field operators, shift supervisors, etc., assess the situation as best they can, and begin following general procedures on which they have been trained.

This can be a daunting task, especially because up until it is turned off, the APC has been pushing the system into the furthest "corners" of the multidimensional optimization space. Often, this means that when one of the optimizer's assumptions is violated, the plant state deteriorates quickly, because it doesn't have far to go to "fall off a cliff." Unfortunately, the operator must often begin the abnormal situation recovery procedure in uncertain proximity to the bottom of that cliff.

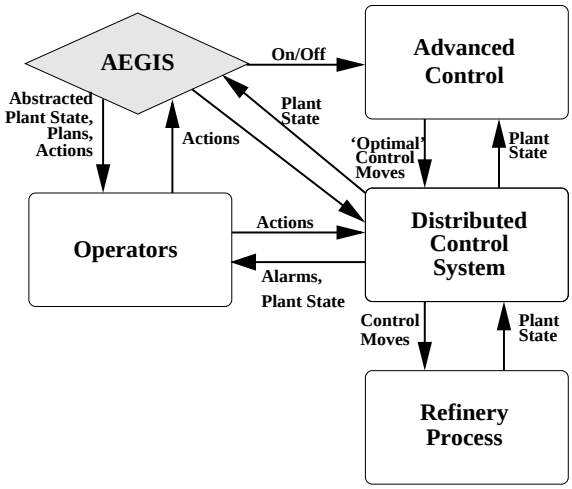

Figure 3: Refinery Control with AEGIS.

What is to be Done?

While we believe that improved human interaction techniques are very important, they are not the key to actually solving the underlying problem, the fundamental incompatibility of humans and automatic control. What is needed is *model-based autonomy*. Rather than having a subordinate control system to be supervised, we must have a full-partner autonomous control system that understands the plant in detail, can access and control many key parameters, and collaborates with the human as a teammate, not a subordinate.

The key here is model-based: the autonomous system must use explicit and detailed plant models to understand the state of the system, the team objectives, and the impact of its actions. If the automation's behavior is based on a sufficiently complex model, the human operator can interact with the automation as he would with another human: cooperating on allocating roles and responsibilities, querying and explaining situation understanding, and trusting the expertise of the teammate. This is not a particularly new idea, it is just difficult.

We were involved in developing this type of model-driven "associate system" for refineries. The Abnormal Event Guidance and Information System (AEGIS) is a large-scale distributed intelligent system designed primarily to improve responses to abnormal situations, both by automating some activities currently performed by operations personnel and by improving human situation awareness. AEGIS performs various functions, including choosing goals, planning to achieve them, executing plan actions, communicating with the user, and monitoring both action completion and new plant developments. Figure 3 shows how AEGIS interacts with the existing system.

These functions interact by exchanging information on shared blackboard data structures. One such blackboard, the Plant Reference Model (PRM), captures descriptions of the refinery at varying levels of abstraction and from various perspectives, including the plant's physical layout, the logical processing unit layout, the operational goals of each component, and the current state and suspected malfunctions, with associated confidence levels.

The PRM is a prime example of the type of shared model we advocate. Because the model is explicit and drives the performance of all automation, it can prevent many of the "stupid automation tricks." For instance, the "foolie" described earlier would no longer be necessary with use of a proper PRM, since violations of operational goals (e.g., maintain 100% air flow), and the relationships between these goals and plant operations (e.g., the temperature sensor/slide valve PID loop assumes that "maintain air flow" is satisfied) would be explicitly represented, communicated to AEGIS components and human alike, and taken into account at the right level of abstraction. This allows the human and automation to stay on the same plane of understanding. Instead of forcing the human to predict the performance of automation and work around it, the human simply expresses new objectives or information and the automation will understand the implications and do the right thing. In our example, the system might detect the combustion air decrease automatically, or the human might make the observation (e.g., "We are losing combustion air (reason unknown)"). Collaboration and reduced operator workload result, instead of the increased workload that now results from the operator's need to think hard about what ignorant but complex automation will do.

References

Leffler, W. L. 1985. *Petroleum Refining for the Non-Technical Person*. Tulsa, OK: PennWell Publishing Company.