نشریه علمی سازمان انرژی اتمی ایران
شماره ۱۳، صفحات ۲۶ـ۲۱، ۱۳۷۶.

به کارگیری مفهوم تحمل خطا در طراحی اتاق کنترل نیروگاههای هسته‌ای

کامران سپانلو
واحد نظام ایمنی
سازمان انرژی اتمی ایران

چکیده

داده‌های مربوط به قابلیت اعتماد انسان در اتاقهای کنترل نشان دهنده پایین بودن این پارامتر است. این امر به ویژه در شرایط دشوار و پیش بینی نشده اضطراری که طی آن عملکرد ضعیف اپراتور می تواند به وقوع فرایندهای مخاطره‌آمیز و برگشت ناپذیر منجر شود، اهمیت دارد. امروزه براساس تحقیقات گسترده در زمینه نقش انسان در سیستمهای تکنولوژیک معلوم شده است که نمی توان به روشهای سنتی و متداول، خطای انسانی را به طور کامل از محیطهای متغیر، قابل انعطاف و مدرن، نظیر نیروگاههای هسته‌ای حذف کرد. در این مقاله، مفهوم روش تحمل خطا در برخورد با خطای انسانی بررسی شده و ویژگیهای آن در پشتیبانی فعالیتهای ذهنی اپراتورها، حین شرایط نامعلوم در نیروگاههای هسته‌ای، بیان شده است.

مقدمه

خطای انسانی به عنوان علت اصلی حوادث در سیستمهای تکنولوژیک پیچیده شناخته شده و این امر به توجه روزافزون نسبت به نقش انسان در ایمنی سیستمهای تکنولوژیک منجر شده است. داده‌های مربوط به قابلیت اعتماد اتاقهای کنترل نشان داده است که قابلیت اعتماد انسانی در این مکانها به نحو غیر قابل قبولی پایین است [۱]. این موضوع به ویژه تحت شرایط پیش بینی نشده که در آن کاهش قابلیتهای عملکرد اپراتور می تواند به فرایندهای برگشت ناپذیر منجر شود، اهمیت پیدا می کند. عموما"، باور بر این است که مهمترین وظایف اپراتور تصمیم‌گیری در لحظات بحرانی حین شکل‌گیری یک حادثه است. سیستمهای بزرگ و پیچیده تکنولوژیک موجود، یک سری وظایف جدید برعهده اپراتورها گذاشته است. این سیستمها از اپراتورها انتظار دارند که خود را به طور پیوسته با شرایط جدید و پیش بینی نشده سیستم و نیز با تغییرات محیطی تطبیق و پارامترهای سیستم را هماهنگ با ضرورتهای متغیر بیرونی و نیز دگرگونیهای شرایط محیطی تغییر دهند. به عبارت دیگر، به نقل از Reason [۲]، اپراتورها باید قادر باشند شرایط اضطراری « پیش بینی نشده در طراحی » را کنترل کنند، زیرا طراحان این گونه سیستمها نمی توانند تمامی سناریوهای ممکن خطا را پیش بینی کنند، در نتیجه، تجهیزات خودکار ایمنی و/ یا دستورالعملهای اجرایی برای این شرایط در نظر گرفته نمی شود. بنابراین، این امر بسیار مهم است که کار اپراتور که با فعالیتهای خطاانگیز در حل معضلات و تصمیم‌گیری همراه است به کمک ابزارهای واسطهٔ مناسب آسان و توسط ساختار مورد نیاز سازمانی پشتیبانی شود.

پیامدهای منفی افزایش خودکاری سیستمها

تکنولوژیهای مدرن ریزپردازنده‌ها و سیستمهای کمک تصمیم‌گیری خودکار این امکان را فراهم آورده است تا بسیاری از کارهایی که پیشتر در اتاق کنترل نیروگاههای هسته‌ای توسط اپراتور انجام می شد به طور خودکار انجام شود. خودکاری فایده‌های بسیاری فراهم آورده است. امروزه سؤال این نیست که آیا یک

عمل را «می توان» خودکار کرد یا نـه، بلکـه ایـن است که آیـا «باید» آن را خـودکـار کـرد یـا نـه. ایـن امـر که همواره ایمنی کلی سیستم با اختصاص دادن وظایف ایمنی به سیستمهای خودکار افزایش می یابد بسیار سؤال برانگیز است. به دلایل مختلف، این اعتقاد ایجاد شده است که شاید سطح خودکاری سیستمهای ایمنی اتاق کنترل ازحد «بهینه» خارج شده باشد. تصوری که عموما" از خودکاری وجود دارد به این صورت است که ماشینهای ساکتی هستند که خطا نمی کنند، کارایی آنها بالاست، کاملا" وابسته و خادم انسان هستند و خطاهای وی را حذف می کنند. اما شواهد بسیاری درمورد عملکرد سیستمهای خودکار موجود است که باور مطلق به خودکاری را رد می کنند. برای مثال، مشخص شده است که به طورمتوسط در هر هزار خط برنامه‌نویسی کامپیوتری سه خطارخ می دهد [۳].

همچنین، موارد بسیاری از تاثیر مخرب خودکاری در پروازهای هوایـی وجـود دارد. در صنعت هواپیمایی، ایده خلبان کامپیوتری رد شده است زیرا:

۱ـ دستگـاههـای خـودکـار بـه طـور مـرتب خـراب می شوند.

۲ـ خطاهای تازه‌ای بر اثر کاربرد سیستمهای خودکار بروز می کند.

۳ـ میزان تبحر خلبان در پی کاربرد سیستمهای خودکار تدریجا" کاهش می یابد.

ضمنا" به نظر می رسد که افکار عمومی به همان اندازه که نسبت به خطاناپذیربودن سیستمهای خودکار شکاک هستند از پیامدهای وقوع خرابی در آن سیستمهـا نیـز بیم دارند [۴].

انتظار می رود که اپراتورها به دلیل انعطاف پذیری، توانایی یادگیری، توانایی تطبیق با ویژگیهای سیستـم و علی‌رغـم افـزایـش سطـح بـه‌کـارگیـری کامپیوتر و خودکاری، درآینده نیز همچنان مسئولیت کنترل و نظارت بر سیستمهای تکنولوژیک و پیچیده را برعهده داشته باشند. درواقع از اپراتورها انتظار می رود که «فضاهای خالی ذهن طراحان این گونه سیستمها را پر کنند»[۵].

براساس تجزیه و تحلیل موارد اضطراری واقعی در نیـروگـاههـای هسته‌ای مشخص شـده است که به دلیل طبیعت پیچیده، به هم بسته و بسیار برهم کنشی سیستم، هر رویدادی از ویژگی یگانه‌ای برخوردار است، بنابراین تلاش درجهت تعبیه پاسخهای از پیش تعیین شده خودکار برای حالتهای اضطراری، ایمنی سیستم را تضمین نمی کند [۶]. به این ترتیب سیستمهای ایمنی خودکار برای مقابله با رویدادهای «پیش‌بینی شده تـوسط طـراح» مناسب هستند و تلاشهایی که با به کارگیری سیستمهای ایمنی خودکار درجهـت مهـار خطـر نـاشـی از عملکـرد تنش‌آلـود اپراتورها در شـرایط اضطراری انجام می شود نمی تواند مانع بروز یک خطر بزرگتر شود: این که اپراتورها از پیـش و بـدون اینکـه مطلـع بـاشند توسط خطاهای انجام شده در طی تعمیر، نگهداری و آزمایش این سیستمها «فلج» شده باشند [۷].

فلسفه دفاع در عمق و خطاهای نهفته

دفاع در عمق به طور وسیعی به عنوان فلسفه ایمنی تاسیسات تکنولوژیک پیچیده و مخاطره آمیز پذیرفته شده است. این استراتژی براساس قـرار دادن لایه‌های هم پوشاننده‌ای است که به کمک سیستمهای فعال ایمنی، مواد مخاطره‌آمیز را محبوس نگه میدارد و از نشت آن به بیرون پیشگیری می کند. به علاوه، یکپارچگی لایه‌ها از طریق پیش‌بینی حاشیه‌های ایمنی در طراحی آنها و نیز سیستمهای ایمنی حفظ می شود. کـدری لایـه‌هـای ایمنی از نظر تاثیر خطاهای انسانی بر آنهـا و ظرفیـت تحمل این لایـه‌ها ایـن امکـان را می دهد که تاثیر خطاهای انسانی برای زمان طولانی درون سیستم پنهـان بمـاند. بنابراین، درکنـار فـواید غیر قابل انکار بسیار، این استراتژی تاحدی سیستم را نسبت به خطاهای انسانی و خرابیهای سخت افزاری، «بخششگر» یا به عبارت دقیقتر آسیب پذیر می کند. خطـاهـای نهـان همچنین ممکـن اسـت بـه راههـای گـوناگون دیگـری وارد سیستـم شـونـد. از جمله ایـن

راههـا مـی‌تـوان بـه نقـایص طـراحـی، تـصمیمـات مدیـریتـی نادرست، خطـاهـای تعمیـر و نگهـداری و دستورالعملهای بهره‌برداری ضعیف اشاره کرد. هرچه سیستم پیچیده‌تر و کدرتر باشد، تعداد خطاهای نهفته بیشتر خواهد شد. در بسیاری مواقع اثر این خطاها توسط سیستم، تحمل، آشکار و تصحیح می شود، ولی در برخی شرایـط دیگـر، ایـن خطـاهـا در یک ترکیب غیر محتمل و یگانه با خطاهای مرتکب شده در هنگام بهره‌برداری، موانع دفاعی تعبیه شده دربرابر نشت مواد مخاطره‌آمیز را بی اثر می کند و حوادث ناگوار روی می دهد [۲ و ۶].

سیستمهای متحمل خطا

خطای انسانی هنگامی روی می دهد که اثر رفتار انسان از حـد قابل اغماض خود بگذرد. در بسیاری از مـوارد محیـط کاری نیز باعث تشدید وضعیت بروز خطا می‌شود. در چنین محیط کاری نامناسبی، هنگام روی دادن خطا، امکان تصحیح اثرهای آن برای اپراتور، پیـش از منتهـی شـدن بـه پیـامـدهای غیر قابل جبران وجود ندارد، زیرا تبعات خطا نه قابل مشاهده هستند و نه برگشت‌پذیر [۸]. اخیرا" براساس پژوهشهای گسترده در زمینه شناخت نقش عامل انسانی در بروز حوادث سیستمهای تکنولوژیک، مشخص شده است که باتوجه به شرایط متغیر و انعطاف پذیر این سیستمها، امکان حـذف کـامـل خطـای انسـانی وجـود ندارد. برای فراهم آوردن امکان وقوع و درعین حال مقابله با پیامد خطاهای انسانی در سیستمهای تکنولوژیک بزرگ مانند نیروگاههای هسته‌ای، باید خطاهای انسانی به عنوان تجربه های ناموفق یا غیر قابل قبول انسانها در یک محیط کاری «غیر دوستانه» درنظر گرفته شوند. بنـابـراین، طراحی محیطهای کاری «دوستانه» یا «متحمل خطا» همراه با ساختارهای سازمانی مناسب آن از اهمیت ویژه‌ای برخـوردار مـی شود [۹، ۱۰، ۱۱، ۱۲و ۱۳].

طـراحـی تجهیزات واسطه باید درجهت قابل مشاهده کردن مرزهای رفتاری قابل قبول برای اپراتورها باشد، به گونه‌ای که اثر خطاهای ارتکـابـی بـرای وی مشاهده‌پذیر و برگشت‌پذیر باشند. بـه منظـور یـاری اپـراتـورهـا برای مقابلـه با شرایط پیش‌بینی نشده (ورای دسـتـورالعملهای بهره‌برداری)، طراحـی سیستمـهای واسطـه باید این امکـان را برای اپراتورها فراهم کند که بتوانند فرضیـه‌های خود را درمورد فـرایـنـدهای بالقوه برگشت‌ناپذیر آزمایش کنند، بدون آن که مجبور باشند آنها را مستقیما" به کار ببرند. معمولا" در سازمانها، گروههای مختلف کاری باید به تغییرات سریع پاسخی بدهند که فرصت تجزیه و تحلیل کامل آن را پیش از اقدام ندارند. همچنین، ترکیب تصمیم‌گیریها در بخشهای مختلف در پاره‌ای از موارد به پیامدهای پیش بینی نشده‌ای منجر می شود. ایده تحمل خطا در اینجا اهمیت می یابد، زیرا ناسازگاری بین راه‌حلهای برگزیده توسط گروههای مختلف، می تواند پیامدهای اقتصادی و زیست محیطی گسـتـرده‌ای داشتـه باشد. یک راه حل، ایجاد یک سیستم یکپارچه اطلاعاتی است که ارتباط افقی موثری بین گروهها برقرار کند به طوری که اثر تصمیم‌گیری اعضای یک گروه برای افراد آن و نیز سایر گروهها قابل مشاهده شود. ایده تحمل خطا می‌تواند در جهت دستیابی به هدفهای مطرح شده در طراحی سیستمهای واسطه انسان - ماشین در اتاق کنترل نیروگاههای هسته‌ای به کار رود. برای این کار باید تقسیم وظایف بین گروههای دست اندرکار در هنگام بهره‌برداری نیروگاه تجزیه و تحلیل شود تا افرادی که تصمیمات آنـان بـر عملکـرد موفـق اجـزای کنتـرل موثـر است معـلوم شونـد. همچنیـن باید مکان و شقهـای مختلـف تصمیـم‌گیـری مـوجـود بـرای اپـراتـورهـا (درصورت بروز شرایط اضطراری) و ملاکهـای تصمیم‌گیری راهنمای آنان، مشخص شوند. تعیین شبکه ارتباطی بین تصمیم‌گیرندگان در هنگام پاسخ به شرایط اضطراری نیز اهمیت دارد. شرایط مرزی بهره‌برداری ایمن در مواقع اضطراری باید مشخص شوند تا مشـاهده‌پذیری

و برگشت‌پذیری عبور از حدود امکان پذیر شود. یک سیستم متحمل خطا در اتاق کنترل یک نیروگاه هسته‌ای دارای ویژگیهای همزمان سیستمهای واسطه انسان - ماشین و انسان - انسان است. این سیستمها نوعی سیستمهای واسطه انسان - ماشین هستند زیرا اپراتور از طریق آنها با نیروگاه ارتباط پیدا می کند و عمل می‌کند، و درعین حال نوعی سیستم واسطه انسان - انسان هستند زیرا سایر تصمیم‌گیرندگان را درمورد عملکرد و تاثیر تصمیم دیگران بر قلمروی خویش آگاه می کنند. از طرف دیگر، سیستمهای متحمل خطا را می‌توان نوعی سیستم کمک تصمیم‌گیری نیز دانست، زیرا وضعیت واقعی نیروگاه و پیامدهای اجرای تصمیمهای اپراتور را برای وی روشن می سازد.

سیستمهای متحمل خطا دارای ویژگیهای سادگی، شفاف‌بودن، آشکارسازی خطا و توانایی تصحیح خطا هستند. این سیستمها برای اپراتور امکان درک صحیح از وضعیت واقعی نیروگاه را فراهم می کنند و وضوح عملکرد انسانی در نیروگاه را افزایش می دهند. به این ترتیب، تصمیمهای گرفته شده توسط هر شخص به وسیله ذهن «جمعی» مشاهده و ارزیابی می شود. این امر به میزان زیادی امکان آشکارسازی هرگونه خطا را افزایش می دهد. سرعت عمل سیستم متحمل خطا باید بیش از آهنگ وخامت وضعیت نیروگاه پس از وقوع خطا باشد. زمان مورد نیاز سیستم متحمل خطا برای روشن کردن نادرستی عمل اپراتور نباید آنقدر زیاد باشد که به فرایندهای برگشت‌ناپذیر مجال پیشرفت دهد. به عبارت دیگر، سیستمهای متحمل خطا نباید نیروگاه را در معرض هرگونه خطر ناشی از بی عملی اپراتور درمقابل دینامیک سریع فرایندهای مرتبط با ایمنی قرار دهد. خوشبختانه، بیشتر فرایندهای یک نیروگاه هسته‌ای (برای مثال تحولات ترموهیدرولیک) دارای ثابت زمانی بزرگی هستند که به این سیستمها امکان عمل می دهد.

نتیجه گیری

تطبیق پویا با شرایط محیطی سریع، هم برای رفتار فردی و هم برای تقسیم کار بین افراد می تواند، درصورت مشاهده‌پذیر و برگشت‌پذیر بودن خطاها، با قابلیت اعتماد زیادی انجام شود. مفهوم سیستمهای متحمل خطا راهی است که یک محیط ذهنی «بخشنگر» برای اپراتور فراهم می سازد به طوری که بتواند با شرایط پیش بینی نشده در طراحی مقابله کند.

References

1. E. Hollnagel, Plan Recognition in Modelling of Users. Reliability Engineering and System Safety 22, 129 (1988).
2. J. Reason, Human Error. Cambridge University Press. England (1990).
3. A. Carnino, Man and Risks. Marcel Decker Publisher, New York (1990).
4. E. Wiener, and R. Curry, Flight-Deck Automation: Promises and Problems. Pilot Error, the Human Factors, Second Edition, GRANADA Publication, pp 67-86 (1982).
5. J. Rasmussen, What Can be Learned from Human Error Reports? In K.D. Duncan, M.M. Gruneberg & D. Walls (Eds), Changes in Working Life, New York: John Wiley & Sons, 97-113 (1980).
6. J. Reason, Modelling the Basic Error Tendencies of Human Operators. Reliability Engineering and System Safety 22. pp 137-153 (1988).
7. J. Reason, The Human Contribution to Nuclear Power Plant Emergencies. Conference on Human Reliability in Nuclear Power Plants 22-23, Oct. London (1987).
8. N. Meshkati, Integration of Workstations, Job and Team Sructure Design in Complex Human-Machine Systems: A Framework. International Journal of Industrial Ergonomics 7, 111-122 (1991).
9. J. Rasmussen, Human Error Mechanisms in Complex Work Environments. Reliability Engineering and System Safety 22, 155-167 (1988).
10. J. Rasmussen, The Role of Error in Organizing Behaviour, Ergonomics, Vol.33, Nos. 10/11, 1185-1199 (1990).
11. J. Rasmussen, Risk Management, Adaptation, and Design for Safety. Future Risk and Risk Management. Dordrecht: Kluwer (1993).
12. J. Rasmussen, A. Pejtersen, and L. Goodstein, Cognitive Systems Engineering. John Wiley & Sons (1994).
13. N. Meshkati, A Method for Managing the Integration of Error Tolerant Design in Manufacturing Systems, In Edition (1994).

AEOI Scientific Bulletin
No. 13, PP. 21-26, (1997)

INTEGRATION OF ERROR TOLERANT CONCEPT INTO THE DESIGN OF CONTROL ROOM OF NUCLEAR POWER PLANTS

K. Sepanloo
Nuclear safety Department
Atomic Energy Organization of Iran

Abstract

Data on human reliability in control rooms indicate that human reliability is unacceptably low. This is particularly important under difficult unexpected situations in emergencies where the operator's deteriorated performance may lead to irreversible hazardous processes in the plant. Today, based on extensive research on the role of human element in technological systems, it is known that human error can not totally be eliminated in a modern flexible, changing environment, such as nuclear power plant, by conventional style designs. In this paper the innovative concept of error tolerance has been further explored to be utilized in supporting the cognitive functions of operators during the emergencies in nuclear power plants.