Энергетика, Smart Grid, интеллектуальные транспортные сети.

Практические возможности в России

Продолжаем публикацию материала, в котором рассматриваются практические возможности реализации концепции Smart Grid для энергетических предприятий в России.

Как сложить пазл

Естественно, что Smart-диспетчерские, базирующиеся на цифровых подстанциях, нуждаются в очень надежных сетях связи (IEC 60870-6). Так, крупнейшая энергетическая компания Китая, SGCC, пошла следующим путем, показавшим свою эффективность: оставила старую систему диспетчерских и их систему связи и параллельно начала строить новую информационную диспетчерскую сеть (IDN). Такой подход потребовал разделения энергосети на информационные зоны. В каждой из таких зон применяются свои требования по надежности и безопасности. Конечно, помимо SCADA в проекте появились и другие ИТ- и телекоммуникационные системы, на которые и распространяются эти требования.

Благодаря строительству и развитию сетей Smart Grid обеспечивается дальнейшее расширение энергетических сегментов сети IDN, включая электрические станции и подстанции разных уровней, диспетчерские центры, энергетические блоки, научно-исследовательские институты, центры обслуживания, будущие зарядные станции, а также районы с интеллектуальным энергоснабжением. Сеть IDN становится сетью повсеместного охвата и характеризуется увеличением разнообразия медиауслуг и режимов доступа к услугам, уровня безопасности пользовательского доступа и точности управления на базе пользовательских прав и доменов. Обобщенная архитектура ИТ-коммуникаций при реализации IDN представлена на рис. 5.

Обобщенная архитектура информационного обмена (на примере SGCC) разбивается на несколько сетей, удовлетворяющих всем требованиям в соответствующей информационной зоне: информационная сеть предприятия, сети сбора данных и интеллектуальных датчиков, интеллектуальная сеть на уровне подстанций, комплексная интеллектуальная диспетчерская сеть.

Применение такого подхода к системам связи, по опыту SGCC, позволяет получить и определенный экономический эффект не только для энергосистемы в целом, но и на уровне самих систем связи.

Естественно, что при проектировании, построении и эксплуатации систем связи для энергетической системы также необходимо использование ГИС на CIM-базе. Столь же важным и полезным оказывается применение всего комплекса существующих стандартов. Разумеется, в этой части уже должны быть реализованы требования государственных регуляторов по безопасности критически важной инфраструктуры.

Рис. 5. Надежный и защищенный обмен информацией на всех уровнях – основа Smart Grid

Сборка пазла. Слон уже не так велик

К настоящему времени предложен ряд дорожных карт и архитектур построения сетей Smart Grid. Приведем в качестве примера все тот же Китай, а также упомянем США и Европу.

Государственная электросетевая информационная и телекоммуникационная компания (State Grid Information & Telecommunication Company – SGIT) является дочерним предприятием Государственной электросетевой корпорации Китая (State Grid Corporation of China – SGCC). SGIT отвечает за развитие и эксплуатацию информаци-

Окончание. Начало в REM № 1, 2014

онной и телекоммуникационной инфраструктуры корпорации, а также осуществляет исследования и разработки в области информационных и телекоммуникационных технологий для построения интеллектуальных магистральных и распределительных электросетей. Деятельность SGIT связана с проектированием и научными исследованиями, а также производством оборудования для построения интеллектуальных электросетей.

В изложении SGCC, флагмана энергетической сферы КНР, Strong/Smart Grid звучит как "надежная интеллектуальная сеть". С сетью сверхвысокого напряжения в качестве опорной, и сетями более низкого уровня, работающими как единое целое, китайская Strong/Smart Grid является уникальной, независимой и инновационной разработкой. Это современная система, основанная на ИТ-технологиях и построенная на принципах глубокой автоматизации. "Надежность" и "Интеллектуальность" – два основных принципа, лежащих в ее основе. "Надежность" – это базис системы, в то время как "Интеллектуальность" – основной ориентир. Оба принципа распространяются на все части национальной энергосистемы – от производства, транспортировки, преобразования и до распределения энергии, а также на коммуникационную и информационную платформы, в комплексе осуществляющие интеграцию энергетических и информационных потоков.

Естественно, вся работа строится на ранее разработанной дорожной карте по модернизации сети SGCC. Процесс модернизации этой сети включает три фазы работ (рис. 6), находящихся на разной стадии реализации.

В результате выполнения пилотных и опытных работ возникла приближенная к практике архитектура в виде Интегрированного Центра Управления – масштабируемой платформы для нескольких предметных областей (рис. 7). Центр строится на основе ряда принципов: открытость, стандартизация, визуализация, надежность, безопасность, сервис-ориентированная архитектура. Как и в любой критически важной инфраструктуре тут необходимо учесть резервирование и другие способы обеспечения надежности работы от подстанции до центра через межрегиональное взаимодействие (рис. 8).

Рис. 6. Модернизации сети: фазы работ от SGCC

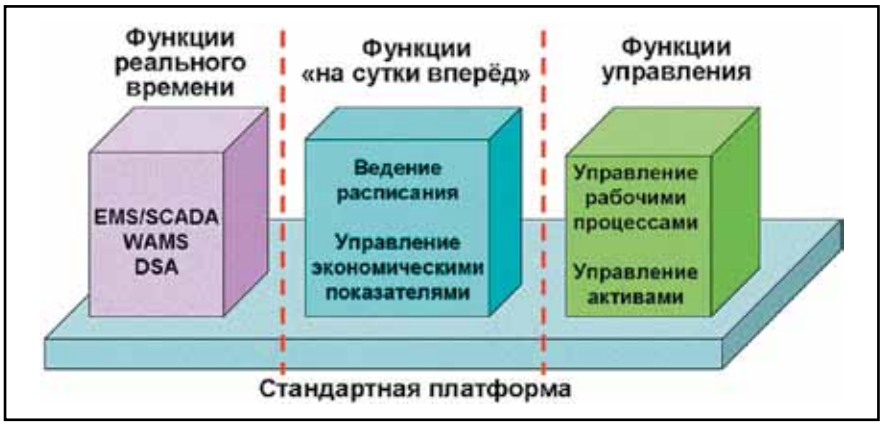

Рис. 7. Общая структура Интегрированного Центра Управления

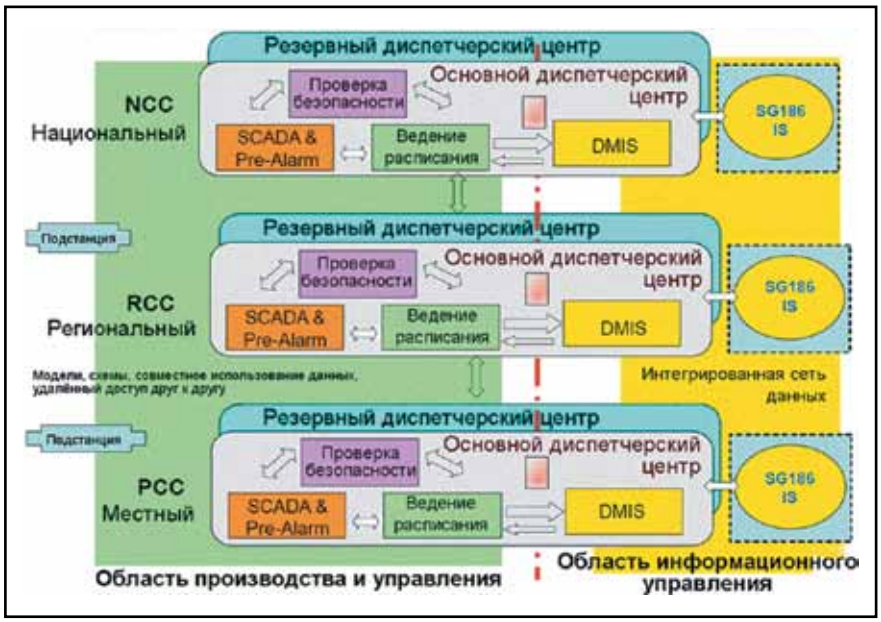

Рис. 8. Интегрированный Центр Управления – обеспечение надежности

При реализации Strong/Smart Grid в качестве стандарта используются CIM-модели, имеющие региональные особенности, но построенные по единой методологии. Это позволяет таким моделям работать от подстанции до диспетчерского центра по всей территории Китая. Такой подход получил название Интегрированной Технологии Моделирования.

Что касается опыта США и Европы, то там также развиваются совместные пилотные проекты по Smart Grid, призванные максимально охватить все аспекты внедрения данных технологий. На портале EPRI приведены сводные данные, показывающие развитие ряда проектов по Smart Grid в США и ЕС. Они хорошо подтверждают тот факт, что приоритеты реализации проектов Smart Grid в энергетических компаниях могут быть разными, но вектор постоянного развития данного направления очевиден.

Таким образом, на международном уровне "пазл Smart Grid" приобретает зримые очертания (рис. 9). Очевидно, что в ряде стран, в частности в Китае, имеются достаточно успешные признаки того, что ситуация позволяет уже "есть слона по частям".

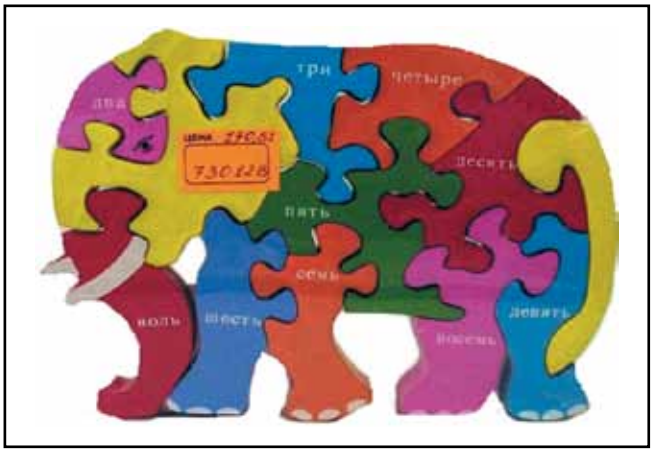

Рис. 9. Пазл Smart Grid

Российским энергетическим компаниям также предстоит выбрать свой путь построения Smart Grid, и авторы надеются, что эта статья может быть им полезна. Поскольку часть "пазла Smart Grid" находится в стадии пилотирования либо уже реализована и реально эксплуатируется, имеется хорошая возможность начать реализацию технологий Smart Grid в России отнюдь не с ненулевой отметки. А огромное количество "пилотов" Smart Grid не должно смущать – это метод тонкой настройки на бизнес-условия конкретной энергетической компании.

В 2011 году IEEE (профильная по ИТ и коммуникациям международная организация стандартизации) опубликовала два практически важных стандарта по теме Smart Grid:

- IEEE Std 1547.4-2011 (Основы разработки, эксплуатации и интеграции автономных систем на базе распределенных ресурсов с электроэнергетическими системами);
- IEEE 2030-2011 (Руководство IEEE по обеспечению функциональной совместимости энергетического оборудования и информационных технологий с электроэнергетическими системами (EPS), системами конечных потребителей и нагрузкой в интеллектуальных сетях).

Важно, что в указанных стандартах появились фактические комплексные показатели эффективности и оценки рисков. Риски создают угрозу ущерба, в отношении которого необходимо принимать меры защиты. Если рисков нет, то и меры безопасности не нужны. Однако когда обнаруживается риск, необходимо определить уязвимые места и угрозы.

В оценку рисков входит анализ имущества, определение ценности информации и имущества, нахождение уязвимых мест и потенциальных рисков, разработка мер по снижению риска и решения, связанные с признанием, предотвращением или передачей рисков. Все эти действия выполняются группой по анализу рисков. Оценка рисков применяется к информации, данным связи и полномочиям. На этом этапе должны быть определены критически важные активы.

Оценка рисков имеет целью определение степени воздействия в случае нарушения безопасности, например, для определенной системы или среды. Риски могут классифицироваться следующим образом:

- ***Риски безопасности*** (могут привести к смерти, серьезным травмам, повреждению оборудования или повреждениям в среде).
- ***Информационные риски*** (могут привести к отказу системы в целом, например потере критически важной инфраструктуры или данных).
- ***Коммерческие риски*** (могут привести к серьезным экономическим затратам, потере бизнеса или репутации).
- ***Риски безопасности информации*** (приводят к потере конфиденциальных данных).

Группа по анализу рисков должна состоять из персонала основных отделов организации – руководства, инженеров, специалистов по безопасности, контролеров процессов, ИТ-специалистов, аналитиков и программистов. Все члены группы должны хорошо разбираться в своей области в части понимания процессов, бизнес-целей, технических принципов, технологий и ситуаций.

Ценность информации и активов

При оценке значимости информации применяются те же критерии, что и при оценке ценности средств, систем, услуг, ресурсов, поставок и персонала. Информация и активы могут быть оценены по качеству и количеству. Активы могут быть как материальными (компьютеры, устройства, сети, системы, помещения, материальные средства), так и нематериальными (репутация, данные, интеллектуальная собственность). Ценность материальных ресурсов определяется по стоимости их приобретения, разработки и обслуживания. Ценность нематериальных активов определяется по степени их важности для владельцев, авторизованных и неавторизованных пользователей.

Определение угроз

Оценка угроз – это в большинстве случаев весьма трудоемкая задача. Угрозы подразделяются на человеческие (намеренные и ненамеренные) и стихийные бедствия. Большинство угроз являются следствием разных уязвимостей, что может привести к самым разным последствиям. Как только для приложений, систем, бизнес-единиц или организаций определена угроза, долж-

но быть проведено обследование всех имеющихся у них уязвимостей.

Определение уязвимостей

Уязвимость – это потенциальная лазейка в системе безопасности, через которую возможны атаки, а также свойство системы или ее среды, которое в сочетании с внутренними или внешними факторами угрозы могут привести к нарушению системы безопасности. Уязвимость характеризуется трудностями и уровнем навыков, который требуется для устранения этих трудностей. При определении конкретных уязвимостей необходимо найти все точки доступа к корпоративной информации (как на электронных, так и физических носителях), например Интернет-соединения, точки удаленного доступа, каналы связи с другими организациями, физический доступ к помещениям, точки пользовательского доступа, точки беспроводного доступа. Для определения уязвимых мест применяются специальные методы анализа способов нарушения безопасности, функциональных сбоев, оцениваются причины таких нарушений и урон, который они способны нанести.

Методики анализа рисков

В настоящее время для обычных ИКТ-систем и для вновь появляющихся структур используются разные методы и концепции оценки. Проектировщики и пользователи систем управления должны оценить пригодность, преимущества и экономичность этих структур. С другой стороны, управление рисками систем управления отличается от управления рисками, принятого для бизнес-систем.

Этапы анализа рисков определены стандартами и методологиями, опубликованными NIST, ISO/IEC и пр. В арсенал способов оценки риска могут входить следующие методы:

- анализ по контрольным листам;
- причинно-следственный анализ;
- иерархическое голографическое моделирование;
- анализ дерева неисправностей;
- анализ дерева событий;
- анализ дерева атак, в том числе на основе возможностей;
- анализ дерева уязвимостей;
- анализ воздействия и критичности нарушений режимов безопасности.

Перечисленные методы могут применяться для оценки рисков в разной среде с определенными ограничениями. Оценка рисков обязательна для определения уровня контроля, необходимого для безопасной работы систем управления мощностью, в которых имеется ценная, конфиденциальная или критически важная информация. Очень важно, чтобы процессы анализа или оценки рисков были хорошо поняты и своевременно исполнялись.

При оценке рисков систем управления мощностью необходимо разработать общие и индивидуальные подходы, которые включают в себя ряд действий по определению рисков, связанных с надежностью и безопасностью энергосистем, персонала, других активов, рассмотрение сценариев типа "что, если...", анализ уязвимостей систем управления, учет ценности активов на основе критериев критичности и неуязвимости и т.д. Также необходимы решения для отслеживания кибер-атак и их прогнозирования с применением данных, собранных специальными устройствами и программами, использования принципов локальности с целью минимизации возможного ущерба.

Суммарный риск или остаточный риск

Между суммарным и остаточным риском существует важная разница, так что организации придется решить, к какому из них она больше готова. Суммарный риск – это функция угроз, уязвимостей и ценности активов. Остаточный риск – это часть риска, которая остается после принятия всех мер противодействия элементам или источникам суммарного риска.

Обработка и уменьшение рисков

Управление информационной безопасностью включает в себя процесс определения приоритетов, бюджета и, наконец, выполнения и поддержания соответствующих мер по снижению риска. После определения размеров суммарного или остаточного риска руководство решает, какие выполнить действия с риском и как его уменьшить. Риск может быть передан, отклонен, принят или уменьшен.

Если организация принимает решение прекратить деятельность, создающую риск, это называется "исключение риска". "Уменьшение риска" – подход, при котором риск снижается до уровня, допустимого для продолжения бизнес-деятельности. К способам уменьшения рисков относится применение разных технологий безопасности. "Принятие риска" используется, когда затраты на меры противодействия перевешивают потенциальные убытки либо основывается на таких факторах, как соображения безопасности, экологические и рабочие характеристики.

Кроме того, люди, участвующие в управлении рисками в разных функциональных областях, должны быть способны обмениваться знаниями. Поэтому одна их характеристик успешной программы управления рисками включает в себя механизмы, упрощающие такое взаимодействие.

Надежность

Надежность – это способность компонента или всей системы выполнять свои функции в предусмотренных условиях в предусмотренный период времени (IEEE Std 493-2007 [B11]). Сложность архитектуры интеллектуальных сетей создает определенные трудности для обеспечения их надежности, которых в сегодняшних условиях можно было бы избежать. Аналогично, размеры и географический размах воздействия отказа сетей, несомненно, растут по мере распространения сложных архитектур и средств связи в электроэнергетических системах (EPS).

Чтобы эффективно выработать требования по надежности, необходимо понимать, что в сфере энергетики и в ИКТ-отрасли понятие надежности охватывает широкий круг вопросов, охватывающих обеспечение надежности электроэнергии, надежность передачи данных, итеративный характер проектирования, работу оборудования интеллектуальных энергосетей в нештатной ситуации.

Инженеры-электроэнергетики прежде всего думают о мерах надежного энергоснабжения потребителей. Но для поддержки применения интеллектуальных энергосетей необходимо позаботиться также о надежности передачи данных. Таким образом, один ряд мер должен быть направлен на обеспечение надежности электроснабжения, другой – надежности данных. Несмотря на использование разных мер для достижения надежности инфраструктуры EPS и ИКТ безопасность и надежность энергосистем в случае нарушений в ИКТ-инфраструктуре должны иметь приоритетную значимость.

Надежность энергоснабжения

В распределительных системах надежность электроснабжения обычно измеряется в показателях надежности (IEEE Std 1366 [B12]), например SAIDI (средний показатель аварий в системе), SAIFI (средний показатель частоты аварий в системе).

Очень часто эти показатели используются регулирующими органами для оценки надежности электроснабжения, обеспечиваемого электросетями. Они включают в себя показатели распределения, передачи и генерации электроэнергии. Обычная цель любого коммунального предприятия – сохранять эти значения на минимально допустимом уровне. Так как некоторые из этих мер могут не предусматривать отказы, вызванные погодными условиями, должны использоваться критерии оценки электроснабжения, включающие в себя все данные об отказах и ремонтах.

Интеллектуальные энергосети в потенциале способны улучшить надежность энергораспределения. Для этого через каналы передачи данных на базе ИКТ должны предоставляться различные данные управления и данные от сенсорных систем. Для некоторых маршрутов передачи прикладных данных требуется сверхвысокий уровень управления (например, устранение неисправностей и автономное восстановление энергоснабжения), в то время как большинство приложений способно выдерживать сравнительно продолжительные или частые прерывания без негативного воздействия на надежность энергоснабжения (например, считывание электросчетчиков). Для энергетиков очень важно четко согласовать меры надежности, чтобы избежать ненужных затрат на ИКТ, а также избыточных аварий в энергосистеме.

Надежность данных

Надежность определенных потоков данных является основным требованием, которое должно быть предусмотрено для энергосистем. Процесс разработки конкретных критериев для определенного потока данных является итеративным. Энергетика и ИКТ-отрасль должны совместно определить оптимальную реализацию интерфейсов и каналов для передачи потоков данных.

Этот уровень надежности учитывается ИКТ при разработке рабочих спецификаций. Используемые показатели надежности и возможные диапазоны значений должны быть поняты всеми, чтобы этот процесс работал эффективно.

Надежность связи

Инженеры-энергетики должны быть способны переводить требования по надежности электроснабжения, которыми они пользуются, в характеристики надежности данных, которыми пользуются ИКТ-системы, и наоборот. Входные данные для расчета надежности электроснабжения можно структурировать с использованием стандартных в области энергетики понятий: продолжительность аварии и частота аварий. В контексте интеллектуальных электросетей потеря данных необязательно вызывает прекращение электроснабжения, но приводит к разбросу значений.

Очень важно понимать, что в любое время, когда согласованные расчетные критерии для потоков данных не соблюдаются, это считается прерыванием (или "потерей" данных). Например, если время передачи информации для определенного потока данных задано как 1,0 с, но данные передаются только через 1,3 с, это будет считаться прерыванием даже в том случае, если данные переданы точно. Соответственно, способность приложений интеллектуальных энергосетей выдерживать потерю или задержки данных можно назвать "устойчивостью к потере данных".

Реальная среда

При оценке надежности и характеристик производительности информационных и компьютерных технологий очень важно учитывать воздействие реальной среды. На производительности некоторых каналов передачи данных могут, например, сказаться следующие факторы:

- погодные условия (ураганы, молнии и др.);
- электромагнитные помехи при природных и антропогенных воздействиях;
- проблемы обеспечения безопасности (как в кибернетическом, так и в физическом пространстве);
- несчастные случаи;
- географические факторы (расстояние, рельеф, топография и т.д.);
- крупномасштабные бедствия (землетрясения, ураганы, лесные пожары и т.п.).

Подобные факторы следует принимать во внимание и при анализе возможных причин сбоев и аварий при передаче данных, а также в процессе определения показателей надежности и рабочих характеристик запланированных каналов передачи данных.

Электромагнитная совместимость

Чтобы максимально реализовать возможный потенциал интеллектуальных энергосетей, они должны быть не менее надежны, безопасны и отказоустойчи-

вы, чем существующие энергосистемы. Для достижения необходимого уровня надежности, нужно решить ряд вопросов. Один из основных вопросов – обеспечение электромагнитной совместимости (ЭМС), которая означает способность выдерживать электромагнитные излучения (с достаточной степенью устойчивости) без создания помех (нарушений) для других сетей и устройств. Электромагнитные помехи разного вида, воздействующие на электросети из разных источников, приводят к ухудшению рабочих характеристик, авариям, выключениям и даже крупномасштабным отказам всей системы.

Чтобы интеллектуальные энергосети нормально функционировали и сосуществовали с другими электрическими и электронными системами, они должны проектироваться с учетом электромагнитных излучений самих сетей и с достаточной степенью устойчивости к различным электромагнитным явлениям вблизи сетей и счетчиков, которые контролируют сети, а также пользовательских интерфейсов.

Аварийный режим работы

Базовым фактором надежности в интеллектуальных энергосетях является соблюдение концепции аварийного режима работы, которая обеспечивает безопасную подачу электроэнергии потребителям в случае отказов системы в части связи. Эта концепция важна для событий, которые оказывают влияние на надежность местной подачи электроэнергии, и для событий регионального масштаба с низкой вероятностью, но высокой степенью влияния. Но более важно то, что поддержка такого аварийного режима на всех уровнях интеллектуальных энергосетей снизит потребность в непомерных затратах на сверхнадежные интерфейсы. В процессе определения требований к потокам данных необходимо учитывать способность системы выдерживать определенные сбои в аварийном режиме.

Заключение

В данной статье не ставилось целью отразить все аспекты темы Smart Grid и роли геоинформационных систем при создании и эксплуатации "умных энергосетей". Между тем, необходимо отметить, что ГИС являются неотъемлемой частью общего процесса, что объясняется уникальными возможностями этой технологии по сбору разнородных данных из различных источников (датчиков, сенсоров, других информационных систем), их обработке и представлению с точной привязкой к местности в удобном для понимания и принятия решений виде.

А. В. Конев, ФГБУ "Российское энергетическое агентство",
В. П. Куприяновский, компания Esri CIS,
А. Ю. Бадалов, "Российская корпорация средств связи",
А. Г. Богданов, компания Huawei,
С. А. Волков, компания Астерос,
С. А. Синягов, компания DATA+

В рамках форума «Российский промышленник»
www.promexpo.lenexpo.ru

Санкт-Петербург
1-3 октября 2014 г.

ПРОМЫШЛЕННАЯ И ВСТРАИВАЕМАЯ ЭЛЕКТРОНИКА 2014

3-я российская специализированная выставка

Электронные модули и системы для промышленной автоматизации бортовых и встраиваемых применений

WWW.INDUSTRIAL-EMBEDDED.RU